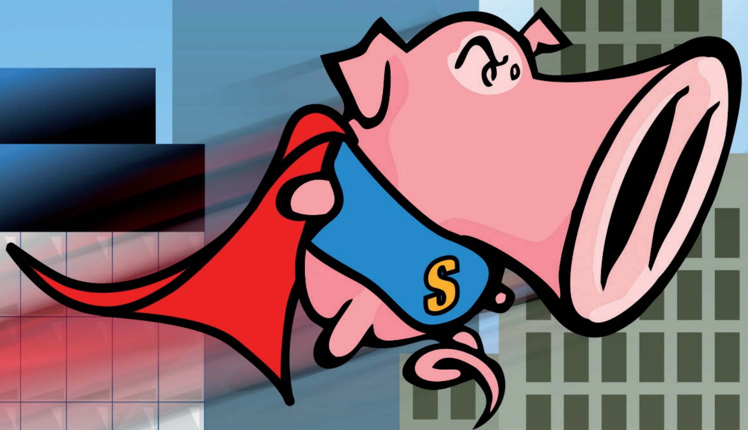
all rights reversed HACKER

Σεπτέμβριος 2014 # Τιμή τεύχους 4€

τεύχος 036 - Bárðarbunga Edition



Εντοπισμός εισβολέων στο επίπεδο του router [*]

Φτιάξτε το δικό σας WiFi Pineapple

Chat, voice και video calls – εντελώς ανώνυμα!

Βολικοί installers για τα προγράμματα σε Python

Ανάλυση αποτελεσμάτων του Snort, μέσα από το Snorby

[*] Με τη βοήθεια του Snort, φυσικά ;)

all rights reversed

HACKER

Περιεχόμενα

και οδηγίες χρήσης

Εκδότης / Διευθυντής	Χρήστος Βαρελάς
Αρχισυντάκτης	Παναγιώτης Βαρελάς
Σύμβουλοι έκδοσης	Νίκος Μουρατίδης, Βούλα Παυλίδου
Σύνταξη	Γιώργος Αραβίδης, Παναγιώτης Βαρελάς, Χρήστος Βαρελάς, Ανδρέας Βενιέρης, Γιώργος Γιάννου, Μανώλης Κιαγιάς, Ιωάννης Κονιάρης, Πέτρος Κυλαδίτης, Γιώργος Μελέκος, Νίκος Μουρατίδης, Θωμάς Σερμπίνης, Νικόλαος Σηφάκης, Μέσος Παπαδόπουλος (TM), Χρίστος Τόμπρας
Γραμματική επιμέλεια	Βούλα Παυλίδου
Καλλιτεχνική Επιμέλεια	Πέτρος Φιλιππίδης

Το ηλεκτρονικό περιοδικό deltaHacker είναι συνδρομητικό και εκδίδεται από την Parabing Creations δώδεκα φορές το χρόνο, κάθε μήνα. Η Parabing Creations έχει την έδρα της στη Μαιώτιδος 3, 55133, Καλαμαριά. Ο δικτυακός τόπος του περιοδικού είναι στο http://deltahacker.gr. Το email επικοινωνίας είναι το talk2us@deltahacker.gr και ειδικά για τις συνδρομές είναι το subscriptions@deltahacker.gr. Οι γενικές πληροφορίες για τις συνδρομές παρατίθενται στο http://deltahacker.gr/subscriptions και οι ίδιες οι παραγγελίες γίνονται από το http://deltahacker.gr/pdf12order. Όλες οι απόψεις που εκφράζονται στα άρθρα δεν εκφράζουν απαραίτητα και τη γνώμη του περιοδικού.

Καζίκια που πέρασαν και σχέδια αντί για πάρτυ

Αρκετοί φίλοι σίγουρα θα το προσέξουν, οι περισσότεροι μάλλον όχι: Με το τεύχος 036 γινόμαστε τριών ετών και σε λίγες εβδομάδες μπαίνουμε, αισίως, στο 4ο έτος κυκλοφορίας του περιοδικού deltaHacker. Θα έπρεπε να το γιορτάζουμε, να οργανώνουμε συναντήσεις και πάρτυ, να γράφουμε λογύδρια ευλογώντας τα γένια μας, να μοιράζουμε ευχαριστίες και υποσχέσεις για το λαμπρό μέλλον που ξεδιπλώνεται μπροστά μας κ.λπ. κ.λπ. Ναι, εντάξει, μερικά τουλάχιστον απ' αυτά θα μπορούσαμε να τα κάνουμε — και κάποια στιγμή θα τα κάνουμε. Τον τελευταίο καιρό, ωστόσο, έχουμε αλλού το μυαλό και την προσοχή μας.

by subZraw

Πέρασε όλο το καλοκαίρι και δεν ετοιμάσαμε ούτε ένα deltaCast. Τα deltaCasts, για τους 5 ή 6 στον πλανήτη που δεν γνωρίζουν ακόμα, είναι τα video tutorials του περιοδικού deltaHacker. Δείτε αν θέλετε τη λίστα με όσα έχουμε ετοιμάσει ως τώρα: `http://deltahacker.gr/category/deltacast`. Όταν μιλάμε για video tutorials, φίλες και φίλοι, εμείς τουλάχιστον δεν εννοούμε ξεπακεταρίσματα προϊόντων, ούτε "παραγωγές" διάρκειας 10, 20 — άντε και 30 λεπτών. Πολύ περισσότερο, τα video tutorials που μας αρέσει να ετοιμάζουμε είναι εκτενή, αναλυτικά, διαρκούν γύρω στη μία ώρα έκαστο και μερικά μάλιστα έχουν φτάσει τις δύο ώρες. Ας πούμε και κάτι ακόμα, επίσης για τους 5 ή 6 στον πλανήτη που δεν γνωρίζουν: Η θεματολογία των deltaCasts συγγενεύει με τη θεματολογία του περιοδικού. Συγκεκριμένα, στα video tutorials ασχολούμαστε με θέματα ethical hacking, networking, security και privacy. (Ίσως και με άλλα, τα οποία όμως δεν θυμάμαι τώρα. Δεν βαριέστε, αμελητέο το κακό.)

Έπαιξαν διάφορα καζίκια το καλοκαίρι που μας πέρασε, που λέτε, για τα οποία ο γράφων δεν έχει το ελεύθερο να πει ή να γράψει κάτι. Και να είχε το ελεύθερο, δηλαδή, πάλι θα απέφευγε την όποια (συγκεκριμένη) αναφορά. Τι τα θέλετε, κάποιες περιπέτειες και καταστάσεις που ταλαιπωρούν —ή έστω τρολλάρουν δυνατά κι ασταμάτητα— τον κοσμάκη, όταν επιτέλους τελειώνουν, μερικοί δεν θέλουμε καν να τις θυμόμαστε. Αλλά δεν θέλω να γενικολογώ για πολλή ώρα ακόμα. Λέω μόνο ότι πλέον όλα είναι καλά και κυλούν (και πάλι) ομαλά. Αυτό.

Εκτός από τη διαρκή φροντίδα για τη μηνιαία κυκλοφορία του deltaHacker, μέσα στο καλοκαίρι κάναμε μερικές παρασκηνιακές προετοιμασίες για το Parabing, την αγγλική εκδοχή του περιοδικού, ενώ ετοιμάσαμε κι ένα νέο theme για το site του deltaHacker. Ο καινούργιος δικτυακός τόπος, ο οποίος εμφανισιακά και λειτουργικά θα διαφέρει αρκετά από τον σημερινό, θα βγει στον αέρα μέσα στον Οκτώβριο. Επειδή όμως θα μετακομίσουμε κιόλας, σε άλλο datacenter ενός άλλου VPS provider, αναπόφευκτα θα βιώσουμε κάποιο downtime. Παράλληλα, έχουμε στα σκαριά και μία ή δύο πρωτότυπες προσφορές για τον Οκτώβριο, με αφορμή τα γενέθλια του deltaHacker που λέγαμε. Να σας πω την αλήθεια, δεν έχουμε ακόμα αποφασίσει για το πότε είναι πιο βολικό να συμβεί αυτό το downtime. Η Σύμβουλος Εκδόσεως™ κι ο κος Αρχισυντάκτης™ είναι της άποψης να μετακομίσουμε το συντομότερο δυνατόν, πριν τα μέσα "του μηνού" (όπως χαρακτηριστικά λέει κι ο Θείος Ακάκιος). Η ταπεινότητά μου, από την άλλη, ψιλοαγχώνεται με τέτοιες μετακομίσεις, οπότε αν πάμε στο νέο datacenter προς το τέλος του μήνα δεν θα το πάρω κατάκαρδα. Τέλος πάντων, θα δούμε ποια άποψη περί "κατάλληλου χρόνου" θα επικρατήσει. (Μπορεί και να μην είναι η δική μου — πού να ξέρω;!)

Θα το 'χετε παρατηρήσει κι εσείς: Τελευταία, το ενδιαφέρον των χρηστών για τις κρυπτογραφημένες επικοινωνίες έχει εκτοξευθεί κατακόρυφα. Δεν αναφέρομαι βεβαίως στην πλειονότητα των χρηστών, οι οποίοι είτε αδιαφορούν παντελώς για τέτοια θέματα είτε σκέφτονται πως ό,τι κι αν κάνουν, όποια μέτρα κι αν λάβουν, κάθε φορά που οι "άλλοι" θέλουν τότε άνετα θα διαβάζουν τα emails τους, θα ψάχνουν τα chat logs τους και θ' ακούνε τις συνομιλίες τους. Λογικό, ειδικά αν λάβουμε υπόψη το γεγονός ότι όλοι αυτοί οι παρακολουθούμενοι αποτελούν "high-profile targets", π.χ., επειδή γνωρίζουν κρατικά μυστικά ή ξέρουν τι κάνατε πέρυσι το καλοκαίρι, ξέρω 'γώ.

Αντίθετα, αναφέρομαι στη μειονότητα των χρηστών, οι οποίοι έχουν μια καλή αίσθηση για το τι σημαίνει σύγχρονη κρυπτογραφία και σκέφτονται ότι θέλουν να έχουν την *επιλογή* για ασφαλείς επικοινωνίες. Όχι επειδή σώνει και καλά έχουν σούπερ-μυστικά που δεν θέλουν να διαρρεύσουν, αλλά επειδή η προστασία της ιδιωτικότητας είναι *δικαίωμά* τους — τελεία και παύλα κι ευχαριστώ πολύ.

Στο νέο deltaCast που αρχίζουμε να παράγουμε αμέσως μετά την κυκλοφορία του τεύχους 036, λοιπόν, επιτιθέμεθα κι εμείς στο καυτό και πάντα επίκαιρο ζήτημα "ασφαλές, κρυπτογραφημένο email". Κοιτάξτε, δεν σκοπεύουμε να παρουσιάσουμε κάποια νέα, εξωτική τεχνολογία ή τεχνική. Η αλήθεια είναι ότι το PGP και οι "ανοικτές" του υλοποιήσεις, όπως είναι το GnuPG, εξακολουθούν να 'ναι άριστες για την κρυπτογράφηση email και δεδομένων γενικότερα. Γιατί τότε δεν χρησιμοποιείται ευρέως, π.χ., το GnuPG; Τι είναι αυτό που συμβαίνει ή δεν συμβαίνει, ώστε να 'χει νόημα η παραγωγή ολόκληρου επεισοδίου, με θέμα την κρυπτογράφηση email; Αρκετά συμβαίνουν — κι αρκετά δεν συμβαίνουν. Κατ' αρχάς, λάβετε υπόψη ότι η διαχείριση των κλειδιών ενός συστήματος δημόσιας κρυπτογραφίας, όπως είναι ένα που βασίζεται στο PGP, δεν είναι ό,τι πιο εύκολο ή άνετο. Προκειμένου η δημόσια κρυπτογραφία στο email να αποτελέσει μια καθημερινή πραγματικότητα, κατ' ελάχιστον πρέπει **α)** να επιμορφωθούν όλοι οι ενδιαφερόμενοι και **β)** να μπουν στον κόπο και να εντάξουν τα εμπλεκόμενα εργαλεία στην καθημερινή τους ρουτίνα. Είναι και το άλλο: Το email, ως σύστημα επικοινωνίας, δεν σχεδιάστηκε με γνώμονα την προστασία του περιεχομένου από αδιάκριτα βλέμματα. Η εφαρμογή του PGP στο email αποτελεί λύση ad hoc και, ακόμη κι αν υποθέσουμε ότι αύριο το πρωί όλοι κρυπτογραφούν το email τους, τα metadata κάθε email παραμένουν μη-κρυπτογραφημένα. Κάποιος λοιπόν που έχει βαλθεί και παρακολουθεί το email μου (λέμε τώρα), ναι μεν αδυνατεί να διαβάζει το περιεχόμενο αλλά εξακολουθεί να βλέπει με *ποιους* επικοινωνώ. Μερικές φορές, αυτό είναι ακριβώς ό,τι χρειάζεται ώστε να πληγεί ανεπανόρθωτα η ιδιωτικότητα — και υπάρχουν ήδη δεδικασμένα όπου οι Αρχές έχουν βασιστεί σε metadata για να κάνουν συλλήψεις. Προσέξτε: Δεν προσπαθούμε να αποφύγουμε τις Αρχές για να κάνουμε σκανταλιές, παγαποντιές ή παρανομίες. Αυτό που επιδιώκουμε εδώ είναι η προστασία των επικοινωνιών μας, αφού καλώς ή κακώς (καλώς!) είμαστε από εκείνους που πιστεύουν ότι αποτελεί βασικό ανθρώπινο δικαίωμα.

Βλέπετε, λοιπόν, ότι αν μη τι άλλο έχουμε αρκετό υλικό για *τουλάχιστον* ένα video tutorial περί κρυπτογραφίας, με εφαρμογή στο email. Είναι που δεν αρκούμαστε μόνο στην (απαραίτητη) θεωρία, αλλά μας αρέσει να περνάμε στην πράξη και βεβαίως να κάνουμε και τις απαραίτητες επιδείξεις.

Ούτως ή άλλως ο Οκτώβριος είναι ωραίος μήνας. Με αυτά που έχουμε μπροστά μας να διερευνήσουμε και να ετοιμάσουμε, κάτι μου λέει ότι για κάποιους από εμάς θα είναι *και* ενδιαφέρων μήνας. Μένει μόνο να βρείτε κι εσείς ενδιαφέρουσα τη δουλειά μας — αλλά το πώς επιτυγχάνεται κάτι τέτοιο είναι ένα άλλο, συναρπαστικό πρόβλημα (που ποτέ δεν δικαιούσαι να πεις ότι το έλυσες).

Καλά να είστε, να φυλάγεστε από λαϊκιστές, από αεριτζήδες κι από επαγγελματίες κινδυνολόγους — και τα λέμε ξανά σύντομα :)



ουέλ μέλ

Αγαπητοί μου,

Ξέρω, ξέρω, βδομάδες τώρα έχετε χάσει τον ύπνο σας αδημονώντας να μάθετε αν ακούγεται το "τζι τζι" των τζιτζικιών ή όχι, όταν δεν είμαστε εμείς εκεί να το ακούσουμε. Σας καταλαβαίνω και σας συμπονώ. Κι εγώ στη θέση σας το ίδιο θα αδημονούσα. Μόνο οι συγγενείς και φίλοι, εδώ γύρω, αδιαφορούν.

Τίποτα. Πέρα βρέχει. Λες και δε ρώτησα.

Προχτές Κυριακή, που συνοδεύαμε τον ανιψιό στο αεροδρόμιο, φανταζόμουν ότι θα μιλούσαμε για το θέμα, αλλά μπα.

Ήμασταν στο Χ95, το λεωφορείο που πηγαινοφέρνει τους ταλαίπωρους ταξιδιώτες μεταξύ Συντάγματος και Αεροδρομίου. Το βασικό μας θέμα συζήτησης ήταν αυτό του Σκωτσέζικου δημοψηφίσματος.

Θα το έχετε πάρει είδηση, θέλω να ελπίζω, πως στη Σκωτία θα γίνει δημοψήφισμα για το αν θέλουν (οι Σκωτσέζοι) να είναι κομμάτι του Ηνωμένου Βασιλείου ή όχι. Το έχουν προγραμματίσει για την ερχόμενη Πέμπτη.

Ο ανιψιός έχει ανησυχήσει πολύ με το δημοψήφισμα αυτό και πρέπει να σας πω ότι συμμερίζομαι την ανησυχία του.

Εντάξει, ξέρω, η δημοκρατία, η γνώμη του λαού, και λοιπά και λοιπά. Παρ' όλα αυτά το διακύβευμα είναι πολύ μεγάλο και δεν περιορίζεται μόνο στα των Σκωτσέζων. Το έχουν σκεφτεί καλά;

Βέβαια, θα μου πείτε, αν είσαι Σκωτσέζος δεν έχεις ούτε λόγο ούτε την πολυτέλεια να σε νοιάζει το διακύβευμα για τους άλλους. Σε ενδιαφέρει μόνο το ίδιο το ερώτημα, και το πώς τίθεται αυτό για 'σένα.

Τέλος πάντων. Ούτε Σκωτσέζος είμαι, ούτε το γνωρίζω το θέμα. Δε νομίζω πως έχει νόημα να επεκταθώ. Το ανέφερα μόνο επειδή μονοπώλησε τη συζήτησή μας σε όλη τη διαδρομή από Σύνταγμα προς Αεροδρόμιο, με το Χ95, και έτσι δεν είπαμε τίποτα για τα τζιτζίκια.

Το μόνο άλλο θέμα για το οποίο προλάβαμε κάτι να πούμε ήταν αυτό με το λεγόμενο Ισλαμικό Κράτος και τους Τζιχαντιστές.

Απορούσαμε από πού ξεφύτρωσε τέτοιο φρούτο και πώς και δεν το είχαμε πάρει είδηση τόσον καιρό. Αναρωτιόμασταν πώς θα τελειώσει αυτή η ιστορία.

Θα μου επιτρέψετε, και πάλι, να μην επεκταθώ. Λέω σήμερα να μη σας κουράσω με πράγματα που δεν γνωρίζω καλά. Στο κάτω κάτω έχουν μιλήσει και γράψει για το θέμα τόσοι και τόσοι. Όπου και ν' ανοίξεις, για το Ισλαμικό Κράτος θα διαβάσεις. Ακόμα και στο περασμένο εντιτόριαλ του περιοδικού μας, εδώ.

Όλοι έχουν μιαν ερμηνεία. Όλοι προσφέρονται να εξηγήσουν. Όλοι μάς θυμίζουν κάτι, ξεχασμένο υποτίθεται, που ρίχνει φως στην υπόθεση.

Well I never, που λένε και οι φίλοι μας οι Σκωτσέζοι.

Σνέιλ μέιλ

Εγώ ένα σχόλιο έχω να κάνω, και θα το κάνω στα Λατινικά.

Post hoc ergo propter hoc.

Δεν ξέρω αν το αναγνωρίζετε. Πρόκειται για το "κωδικό" όνομα ενός συγκεκριμένου λογικού σφάλματος.

Κατά το σφάλμα αυτό η χρονική συσχέτιση εκλαμβάνεται ως αιτιακή. Επειδή, ας πούμε, ένα κάποιο συμβάν Α προηγείται ενός άλλου συμβάντος Β, θεωρούμε αυτομάτως ότι το συμβάν Α αποτελεί αιτία του συμβάντος Β. Αυτό δεν ισχύει αναγκαστικά.

Εντάξει, κάποιες φορές ισχύει -- ξερω 'γω αν δεις φωτιά, και μετά δεις καπνό. Αλλά κάποιες άλλες, πολύ περισσότερες, δεν ισχύει.

Το σφάλμα έγκειται συνήθως στην άγνοιά μας για το πόσα και ποια συμβάντα αλληλοσυσχετίζονται -- και πώς. Ενισχύεται από την πεποίθησή μας (πάντα αθεμελίωτη) ότι μπορούμε, ανά πάσα στιγμή, να δούμε ένα πρόβλημα στην ολότητά του, και συνοδεύεται, συνήθως, από άλλα λογικά σφάλματα όπως αυτό της ψευδούς αναλογίας, του ψευδούς διλήμματος, του φαύλου κύκλου και της αμφισημίας.

Παραδείγματα, αν το ψάξετε, θα βρείτε στο γκουγκλ αρκετά. Αλλά αν δεν θέλετε να πάτε μακριά, ρίξτε μια ματιά στις συζητήσεις και ερμηνείες για το Ισλαμικό Κράτος.

Λοιπόν, αυτό που μου φαίνεται πολύ ενδιαφέρον είναι ένα χαρακτηριστικό αυτών των συζητήσεων, που όλες δείχνουν να το έχουν κοινό. Πρόκειται γι' αυτό που είπα και πιο πάνω: Οι άνθρωποι δείχνουν πάντα έτοιμοι να πιστέψουν ότι ένα πρόβλημα μπορεί (δηλαδή "δύναται") να παρατηρηθεί και μελετηθεί στην ολότητά του.

Δεν πειράζει, σου λέει ο άλλος, αν εσύ προσωπικά δεν μπορείς να το κάνεις. Αρκεί που υπάρχει κάποιος --ο μελετητής κύριος Τάδε, το Πανεπιστήμιο Δείνα, η ερευνητική ομάδα ΧΨΖ-- που *μπορεί* να το κάνει. Τελεία.

(Οπότε εδώ πρέπει να προσθέσουμε ένα ακόμα λογικό σφάλμα, αυτό της προσφυγής στην Αυθεντία.)



Λοιπόν, αυτό που συμβαίνει είναι, νομίζω, το εξής.

Όταν εξετάζουμε ένα φαινόμενο, οποιοδήποτε φαινόμενο, το μεταγράφουμε, κατά κάποιον τρόπο, ως σειρά "δεδομένων", "διαδικασιών", "συμβάντων" κ.λπ. Θεωρούμε ότι αυτά αποτελούν την --ας την πούμε-- ουσία του φαινομένου, και πιστεύουμε ότι μελετώντας αυτά μελετάμε το ίδιο το φαινόμενο.

Σου λέει λοιπόν ο άλλος: Κοίτα, δεν λέω μπαρούφες, μιλάω για γεγονότα. Συνέβη το τάδε. Π.χ., οι Αμερικανοί χρηματοδοτούσαν Ισλαμιστές. Γεγονός. Αφού το παραδέχτηκε κι ο Μπους. Δεν το βγάζω από το μυαλό μου.

Στο λέει και το πιστεύει. Είναι πεπεισμένος. Και πείθει και σένα.

Έλα μου όμως που αυτή η απλή φράση, "σου μιλάω για γεγονότα", δεν είναι καθόλου μα καθόλου απλή.

Ας πάρουμε ένα παράδειγμα: Κοιτάω από το παράθυρο και βλέπω ένα αυτοκίνητο να πέφτει πάνω στο στύλο της ΔΕΗ.

Ποιο είναι το γεγονός εδώ; "Μα", θα μου πείτε, "το ότι το αυτοκίνητο έπεσε στο στύλο".

"Τι μου λέτε;" θα σας απαντήσω εγώ. "Και γιατί όχι: 'Ο οδηγός έχασε τον έλεγχο του οχήματος επειδή του αποσπάστηκε η προσοχή'; Και γιατί όχι: 'Η προσοχή του οδηγού αποσπάστηκε, επειδή προσπάθησε να τσεκάρει το κινητό του ενώ οδηγούσε';" Και πάει λέγοντας.

Γεγονότα δεν είναι και αυτά; Όλα είναι γεγονότα (το υποθέτουμε, έστω, για την συζήτησή μας), όμως το καθένα από αυτά είναι διαφορετικό από το άλλο. Κάτι διαφέρει -- η οπτική γωνία, το κέντρο βάρους και λοιπά.

Πώς μπορούμε να αποφασίσουμε τι εξηγεί τι; Πώς μπορούμε να αποφασίσουμε ποια οπτική γωνία είναι η πιο κατάλληλη για την μελέτη της "ουσίας" ενός φαινομένου; Μπορούμε;

Σκεφτείτε το λίγο, αγαπητοί μου, και θα δείτε πως δεν μπορούμε. Πάντα η σκέψη μας βασίζεται σε σχεδόν αυτονόητες προκείμενες έννοιες / προτάσεις / αλήθειες, τις οποίες έχουμε ήδη εμμέσως και σιωπηλά αποδεχθεί.

Παιδιά, όταν κάτι μας φαίνεται αυτονόητο, είναι επειδή έχουμε ξεχάσει τις προκείμενες που δεν ήταν, οι ίδιες, καθόλου αυτονόητες.

Λυπάμαι που σας το χαλάω, αλλά καθαρά γεγονότα, ως τέτοια, *δεν υπάρχουν*. Υπάρχουν μόνο ερμηνείες. Και κάθε ερμηνεία εμπεριέχει ήδη μιαν άποψη για το πώς έχουν τα πράγματα. Κάθε ερμηνεία είναι ήδη μια θεωρία (υπό την έννοια ότι εντάσσεται ήδη σε ένα πλαίσιο κατανόησης του πεδίου στο οποίο λαμβάνει χώρα το φαινόμενο).

Με άλλα λόγια, αν δεν την είχες τη θεωρία, δεν θα είχες ούτε την ερμηνεία, αλλά ούτε καν το "καθαρό" γεγονός.

Αυτό βέβαια δεν είναι καινούργιο. Οι φιλόσοφοι το είχαν επισημάνει από καιρό. Το λένε και το ξαναλένε.

Όμως αφήστε τους αυτούς να λένε. Το σημαντικό εδώ είναι --φαντάζομαι ότι το βλέπετε πλέον-- πως έτσι επανερχόμαστε στο ερώτημα περί "τζι τζι" και τζιτζικιών.

Η απάντηση που ψάχναμε τόσον καιρό, έχοντας χάσει τον ύπνο μας, είναι εδώ. Μας φανερώνεται.

Θα τη συζητήσουμε την άλλη φορά.

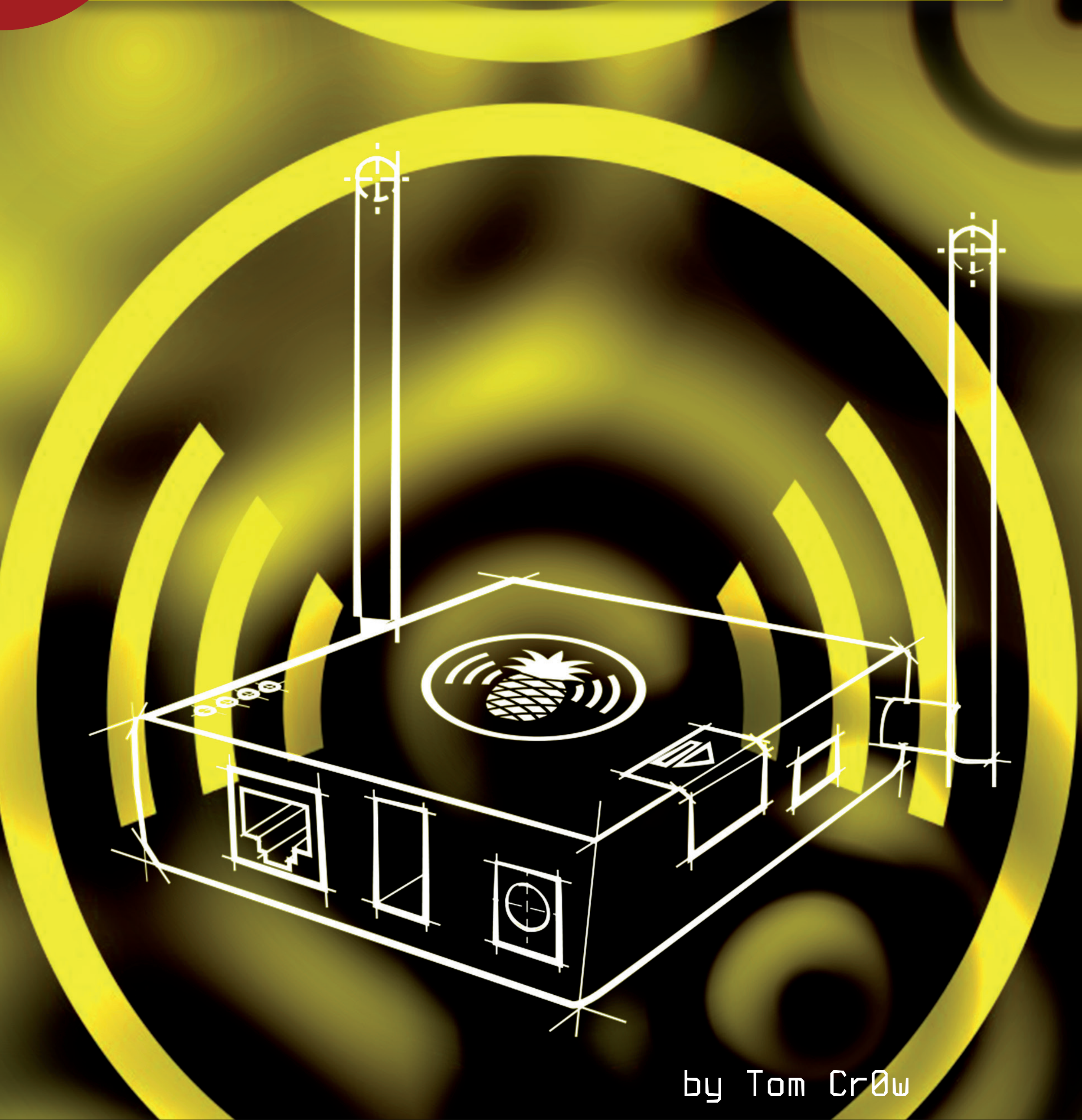
Σας ασπάζομαι,
Θείος Ακάκιος

σουέιμέιγ



A computer is almost human - except that it does not blame its mistakes on another computer.
Είμαστε κοινωνικοί — ειδικά στον online κόσμο.
Είμαστε αστείοι, ευφυείς και φινετσάτοι — ειδικά στον online κόσμο.
Λέγεται ότι έχουμε καβαλήσει το καλάμι — τόσο στον online, όσο και στον offline κόσμο.
Όπως και να 'χει, το διαχειριζόμαστε γενναία.
Περάστε από τα στέκια μας να τα πούμε — ή να μας την πείτε.
twitter.com/deltaHacker
facebook.com/deltaHacker

Skill: Advanced
Tags: OpenWRT, WiFi Pineapple, Alfa AP121U



by Tom Cr0w

Να Άννα ένας ανανάς!

Μας αρέσουν οι ανανάδες! Μας αρέσουν πολύ κι ενδέχεται να το έχετε καταλάβει από καιρό, αφού στο παρελθόν έχουμε αναφερθεί ξανά στο τιτάνιο WiFi Pineapple. Τι θα λέγατε αν αυτή τη φορά φτιάχναμε το δικό μας ανανά; Μην τρομάζετε, δεν θα ασχοληθούμε με τη γενετική τροποποίηση τροφίμων :D

Κάπου στο μακρινό παρελθόν και για την ακρίβεια στο τεύχος 005 του περιοδικού, είχαμε κάνει μια εκτενέστατη παρουσίαση της συσκευής WiFi Pineapple. Για να θυμούνται οι παλιοί και να μαθαίνουν οι καινούργιοι να πούμε ότι πρόκειται για ένα μικρό ασύρματο router, το οποίο έχει τη δυνατότητα ν' αποδεικνύεται ιδιαίτερα επικίνδυνο για τους άλλους. Η μικρή αυτή συσκευή εκμεταλλεύεται τα probe request frames που στέλνουν οι συσκευές WiFi, όταν αναζητούν τα γνωστά σε αυτές δίκτυα. Ο δόλιος ανανάς απαντάει θετικά στα σχετικά ερωτήματα κι εξαπατά τις ανυποψίαστες συσκευές, ώστε να συνδεθούν "επάνω" του. Είναι προφανές, λοιπόν, ότι με το Pineapple υλοποιούνται πανεύκολα ύπουλες επιθέσεις Man-In-The-Middle, οι οποίες είναι δυνατόν να έχουν σοβαρές συνέπειες για τα θύματα. Υπάρχουν πάρα πολλά ακόμα που θα μπορούσαμε να πούμε για τη λειτουργία και τη χρήση του WiFi Pineapple, αλλά στο παρόν άρθρο δεν θα σταθούμε στη θεωρία (αυτό έχει ήδη γίνει). Γι' αυτό το άρθρο έχουμε άλλα σχέδια, πιο δραστήρια.

Τη στιγμή που γράφεται το παρόν άρθρο, ο επίσημος προμηθευτής του WiFi Pineapple διαθέτει την 5η έκδοση της συσκευής (https://wifiPineapple.com). Η συγκεκριμένη έκδοση δεν βασίζεται σε κάποιο router του εμπορίου, όπως συνέβαινε με τις προηγούμενες, αλλά σε μια συσκευή που κατασκευάζεται από τον προμηθευτή[1]. Το ενδιαφέρον σ' αυτή την ιστορία έχει να κάνει με τα παλιότερα μοντέλα και συγκεκριμένα με το firmware που ενσωμάτωναν, το οποίο διατίθεται πλέον ελεύθερα και δωρεάν. Έτσι, μπορούμε να βρούμε το firmware για την αμέσως παλιότερη έκδοση (Mark IV), η οποία βασιζόταν στο router της εταιρίας Alfa και συγκεκριμένα στο μοντέλο AP121U. Έχοντας στη διάθεσή μας το custom firmware, μπορούμε να δημιουργήσουμε το δικό μας WiFi Pineapple, αγοράζοντας μόνο το hardware. Όπως υποψιάζεστε, η απόκτηση ενός ανανά με αυτόν τον τρόπο θα κοστίσει πολύ, μα πολύ λιγότερο ;)

Πριν προχωρήσουμε οφείλουμε να σημειώσουμε ότι σε κάθε έκδοση του Pineapple που έβγαινε κατά καιρούς, το software δεν άλλαζε σε μεγάλο βαθμό. Πέρα από κάποιες αλλαγές στο περιβάλλον (UI) και την προσθήκη διαφόρων add-ons (τα λεγόμενα Infusions, στην ορολογία του ανανά), η λειτουργία του software παρέμενε ίδια. Αυτό που άλλαζε κυρίως ήταν το hardware, το οποίο γινόταν ταχύτερο ή και περισσότερο επεκτάσιμο. Και το λέμε αυτό για να προλάβουμε τις κακές γλώσσες, που θα σπεύσουν να χαρακτηρίσουν την κατασκευή μας ως ξεπερασμένη. Σας διαβεβαιώνουμε ότι ο ανανάς που θα φτιάξουμε (WiFi Pineapple Mark IV) θα λειτουργεί άψογα κι αποτελεσματικότατα.

Απαραίτητο hardware

Όπως είπαμε ήδη, στόχος μας σε αυτό το άρθρο είναι να φτιάξουμε ένα φτηνό WiFi Pineapple, το οποίο θα υστερεί όσο το δυνατόν λιγότερο σε σχέση με την επίσημη συσκευή. Έτσι στραφήκαμε στο hardware της έκδοσης Mark IV (Alfa AP121U), το οποίο προμηθευτήκαμε από το eBay για μόλις 34 ευρώ. Αν αυτή η τιμή σας φαίνεται τσουχτερή, σκεφτείτε ότι η τελευταία έκδοση του Pineapple κοστίζει περί τα 75 ευρώ και το ίδιο ίσχυε για την προηγούμενη.

1. Ο επίσημος προμηθευτής είναι η ομάδα του hak5.org και, όπως καταλαβαίνετε, το ίδιο το hardware κατά πάσα πιθανότητα κατασκευάζεται κάπου στην Κίνα ;)

ΠΡΟΣΟΧΗ: Το μοντέλο που θα αγοράσουμε ΠΡΕΠΕΙ να έχει 8MB flash, 16MB RAM και θύρα USB. Αυτό το τονίζουμε γιατί υπάρχει και το μοντέλο AP121, που δεν έχει θύρα USB, όπως και το μοντέλο AP121U με 32MB RAM και όχι 16MB που *πρέπει* να διαθέτει το δικό μας. Αν επιλέξουμε λάθος μοντέλο, το firmware του Pineapple δεν θα λειτουργεί σωστά και η συσκευή θα είναι άχρηστη για το σκοπό που την αγοράσαμε.

Για να περάσουμε το firmware στη συσκευή μας, θα συνδεθούμε σε αυτήν μέσω της ενσωματωμένης σειριακής θύρας. Στο επίσημο forum του hak5 αναφέρεται ότι γι' αυτή τη δουλειά θα ήταν καλό να χρησιμοποιήσουμε το Alfa Console Board. Ωστόσο, αυτή η συσκευή κοστίζει περί τα 25 ευρώ κι εμείς θεωρήσαμε την αγορά της ασύμφορη. Έτσι, προτιμήσαμε έναν απλό αντάπτορα από USB σε TTL-UART. Για μία ακόμα φορά στραφήκαμε στο eBay και προμηθευτήκαμε μια υλοποίηση με το τσιπάκι CP2102, για μόλις 2 ευρώ! Πρόκειται για μία μικρή πλακετίτσα, η οποία μπορεί να μη σας γεμίζει το μάτι ωστόσο σας πληροφορούμε ότι δουλεύει άψογα. Τέλος, για τη σύνδεση του WiFi Pineapple με τον υπολογιστή θα χρειαστούμε και ένα καλώδιο Ethernet.



Όλο το απαραίτητο hardware, συγκεντρωμένο και τακτοποιημένο, πριν ξεκινήσει το εγχείρημα κατασκευής ενός ανανά! Πρόκειται για το ρουτεράκι AP121U από την Alfa, ένα μικρό τροφοδοτικό, μια κεραία στα 9dBi και ένα καλώδιο δικτύου. Κάτω-κάτω φαίνεται κι ένας μετατροπέας USB 2.0 σε TLL-UART, μαζί με τα συνοδευτικά του καλωδιάκια.

Απαραίτητο software

Όπως αντιλαμβάνεστε, για τη μετατροπή του router σε WiFi Pineapple θα χρειαστούμε το σχετικό firmware καθώς κι ορισμένα εργαλεία, που πρέπει να εγκαταστήσουμε στον υπολογιστή μας. Εμείς εργαστήκαμε σ' ένα σύστημα με Windows 8.1, αλλά η ίδια διαδικασία θα μπορούσε να υλοποιηθεί άνετα και σ' ένα σύστημα με Linux. Ας δούμε τα απαιτούμενα εργαλεία:

- TFTP Server. Για τη μεταφορά αρχείων από τον υπολογιστή προς τη συσκευή θα χρησιμοποιήσουμε μια απλουστευμένη εκδοχή του πρωτοκόλλου FTP, που είναι γνωστή σαν TFTP (Trivial FTP). Συγκεκριμένα, θα στήσουμε στον υπολογιστή μας έναν TFTP server. Για το σκοπό αυτό επιλέξαμε το πρόγραμμα TFTPD32 για τα Windows (http://tftpd32.jounin.net/tftpd32_download.html), ενώ στο Linux θα μπορούσαμε να χρησιμοποιήσουμε το TFTPgui (https://code.google.com/p/tftpgui/downloads/list).

- Secure Copy. Πρόκειται για μία μέθοδο αντιγραφής αρχείων που στηρίζεται στο πρωτόκολλο SSH. Ακριβώς γι' αυτό, τα δεδομένα μεταφέρονται κρυπτογραφημένα και η όλη διαδικασία θεωρείται ασφαλής. Μία άριστη επιλογή για τα Windows αποτελεί το πρόγραμμα WinSCP (http://winscp.net/eng/download.php). Στο Linux δεν χρειάζεται να εγκαταστήσουμε κάτι, αφού το πακέτο OpenSSH είναι πρακτικά στάνταρτ σε όλες τις διανομές και περιλαμβάνει το εργαλείο scp, που πραγματοποιεί τις αντιγραφές (http://linux.die.net/man/1/scp).

- Serial Terminal. Για την αρχική σύνδεση στο WiFi Pineapple θα χρειαστούμε ένα τερματικό που υποστηρίζει συνδέσεις μέσω σειριακής θύρας. Η πιο γνωστή και αξιόπιστη επιλογή για τα Windows είναι το PuTTY (http://www.chiark.greenend.org.uk/~sgtatham/putty), ενώ στο Linux μπορούμε να χρησιμοποιήσουμε το Minicom (https://help.ubuntu.com/community/Minicom).

Σημειώστε ότι δεν είναι υποχρεωτικό να χρησιμοποιηθούν ακριβώς αυτά τα προγράμματα. Αν γνωρίζετε κι εμπιστεύεστε κάποιο άλλο πρόγραμμα για τις δουλειές που περιγράψαμε, μπορείτε κάλλιστα να χρησιμοποιήσετε αυτό. Ας περάσουμε όμως στα απαραίτητα πακέτα με το firmware. Θα χρειαστούμε το αρχικό firmware του router που αγοράσαμε, καθώς και αυτό του WiFi Pineapple.

- AP121U Factory Firmware Files. Το εργοστασιακό firmware του router στηρίζεται σε μια εκδοχή του OpenWRT και απαρτίζεται από δύο αρχεία: Το rootfs.bin και το kernel.bin. Το πρώτο περιέχει όλα τα αρχεία του λειτουργικού συστήματος της συσκευής, ενώ το δεύτερο περιέχει τον πυρήνα και, κατ' επέκταση, όλους τους drivers που απαιτούνται για το χειρισμό του hardware από το software. Αυτά τα αρχεία είναι απαραίτητα για την εργασία μας, αφού θα γραφτούν στη flash της συσκευής εκ νέου. Μπορούμε να τα κατεβάσουμε από εδώ: http://cloud.wifiPineapple.com/mk4/factoryFiles.tar.

- WiFi Pineapple Mark IV Firmware. Το firmware του Pineapple εγκαθίσταται πάνω από αυτό του OpenWRT και μπορούμε να το κατεβάσουμε από εδώ: https://wifiPineapple.com/?downloads&version=mk4. Για το σκοπό μας πρέπει να κατεβάσουμε την έκδοση 2.8.1. Σημειώστε ότι στην ίδια τοποθεσία παρέχεται και η έκδοση 3.0.0, αλλά θα ήταν φρόνιμο να την αποφύγουμε. Η συγκεκριμένη έκδοση αναπτύχθηκε για το hardware του μοντέλου mark V και παρουσιάζει

αρκετά προβλήματα όταν τρέχει στο hardware του Mark IV. Πάντως, αν έχετε όρεξη για δοκιμές και δεν σας ενοχλεί η παρουσία μερικών bugs, θα μπορούσατε να δοκιμάσετε και τις δύο και να κρατήσετε αυτή που σας ικανοποιεί περισσότερο.

Προετοιμασία του hardware

Αρχικά ξεκολλάμε τα δύο πλαστικά ποδαράκια, που βρίσκονται στην κάτω πλευρά της συσκευής και κοντά στη θύρα USB. Έτσι, αποκαλύπτονται δύο βίδες τις οποίες πρέπει να αφαιρέσουμε. Μετά το ξεβίδωμα συνεχίζουμε αφαιρώντας το πλαστικό περίβλημα της συσκευής. Σκοπός μας είναι να αποκτήσουμε πρόσβαση στη σειριακή θύρα (serial port), η οποία δεν έχει την τυπική μορφή (D9-SUB) αλλά παρέχεται ως ένα σύνολο ακροδεκτών. Συγκεκριμένα, πρόκειται για μια τετράδα μεταλλικών προεξοχών, που θα βρούμε στην κάτω πλευρά της πλακέτας και δίπλα στη θύρα USB. Ο ελεγκτής γι' αυτή τη θύρα (UART controller) είναι ενσωματωμένος στο SoC (System-on-Chip) της συσκευής και μεταξύ άλλων επιτρέπει την εγκατάσταση νέου firmware. Σε αυτή τη σειριακή θύρα, λοιπόν, θα συνδέσουμε το μετατροπέα USB 2.0 σε TLL-UART που αγοράσαμε από το eBay.

Κοιτάζοντας την κάτω πλευρά της πλακέτας του AP121U, με τη θύρα USB να είναι στραμμένη προς το δικό μας μέρος, η συνδεσμολογία έχει ως εξής:

1. Ο πρώτος ακροδέκτης από αριστερά είναι το λεγόμενο VDD και προορίζεται για την τροφοδοσία του κυκλώματος. Εμείς *δεν πρέπει* να συνδέσουμε *τίποτα* σε αυτό το pin. Αν προσπαθήσουμε να τροφοδοτήσουμε το κύκλωμα της σειριακής θύρας από τον αντάπτορα, είναι πολύ πιθανό να το κάψουμε και μαζί του να καταστρέψουμε ολόκληρο το SoC. Αυτό σημαίνει ότι η συσκευή μας θα αχρηστευτεί. Τζηζ!

2. Ο δεύτερος ακροδέκτης από αριστερά είναι το RX pin. Όπως υποψιάζεστε, πρόκειται για τον ακροδέκτη υποδοχής δεδομένων (Receive) κι επομένως θα πρέπει να τον συνδέσουμε στον ακροδέκτη αποστολής δεδομένων του μετατροπέα μας. Ο ακροδέκτης που "εκπέμπει" δεδομένα στον μετατροπέα έχει το όνομα TX pin, ενώ σε μερικές υλοποιήσεις ονομάζεται και TXD.

3. Ο τρίτος ακροδέκτης από αριστερά είναι το TX pin. Πρόκειται για τον ακροδέκτη αποστολής δεδομένων (Transmit), τον οποίο θα πρέπει να συνδέσουμε στον ακροδέκτη υποδοχής του αντάπτορα (RX pin ή RXD).

4. Τέλος έχουμε τον ακροδέκτη GND (πρώτος από δεξιά), οποίος πρέπει να συνδεθεί στον ομώνυμο ακροδέκτη του αντάπτορα.

ΠΡΟΣΟΧΗ: Μερικοί μετατροπείς από USB σε TTL-UART αναφέρουν ανάποδα τα ονόματα των ακροδεκτών TX και RX (TXD και RXD). Αυτό γίνεται σκόπιμα από ορισμένους κατασκευαστές, ώστε οι αδαείς χρήστες που θα συνδέσουν τους ομώνυμους ακροδέκτες μεταξύ τους (τον RX με τον RX και τον TX με τον TX) να μη συναντήσουν πρόβλημα. Ευτυχώς, η αντιστροφή της συνδεσμολογίας σε αυτή την περίπτωση δεν είναι καταστροφική. Αν διαπιστώσετε ότι η συνδεσμολογία που περιγράψαμε δεν λειτουργεί, είναι πολύ πιθανό να έχετε πέσει σ' έναν από τους ιδιόρρυθμους αντάπτορες. Η λύση είναι να αντιστρέψτε τη σύνδεση των pin RX και TX.

Το μόνο που μένει τώρα είναι να συνδέσουμε τη θύρα PoE LAN του AP121U με τη θύρα Ethernet του υπολογιστή μας. Κανονικά θα μπορούσαμε να συνδέσουμε και την τροφοδοσία, αλλά όπως θα δούμε στη συνέχεια αυτό είναι προτιμότερο να γίνει την τελευταία στιγμή.



Η συσκευή μας είναι έτοιμη για τη διαδικασία μετατροπής. Το στάδιο που χρειάζεται την περισσότερη προσοχή είναι αυτό της σύνδεσης του μετατροπέα USB σε TTL-UART.

Προετοιμασία του υπολογιστή

Σειρά έχει η προετοιμασία του υπολογιστή από τον οποίο θα εγκαταστήσουμε το firmware του Pineapple στο router μας. Υπενθυμίζουμε ότι εμείς εργαστήκαμε σε σύστημα με Windows. Παρακάτω θα δούμε τις ρυθμίσεις που χρειάστηκε να πραγματοποιήσουμε στο σύστημα.

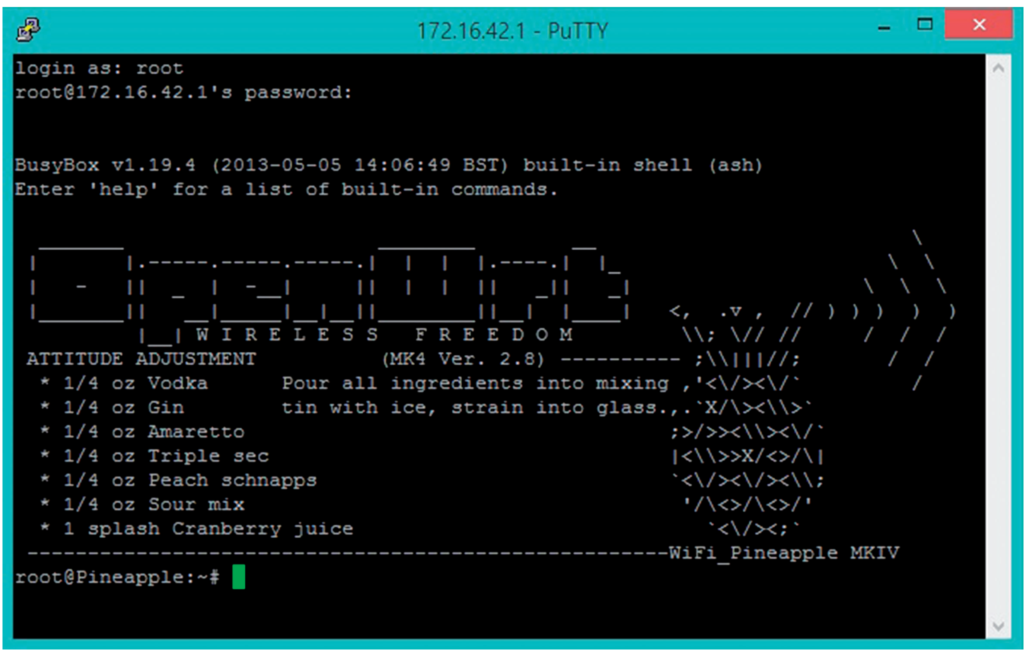
Ξεκινάμε με την κάρτα δικτύου στην οποία έχουμε συνδέσει το "ξεγυμνωμένο" ρουτεράκι μας. Σε αυτή την κάρτα πρέπει να δώσουμε μια στατική διεύθυνση IP και μάλιστα μέσα στο εύρος που προβλέπει το firmware της συσκευής. Αυτό είναι απαραίτητο γιατί ο DHCP του router δεν θα λειτουργεί κατά τα πρώτα στάδια της εργασίας μας και δεν θα μπορεί να μας βοηθήσει. Για το σκοπό αυτό, ανοίγουμε τον "Πίνακα Ελέγχου" κι επιλέγουμε το "Προβολή κατάστασης δικτύου και εργασιών", στην ενότητα "Δίκτυο και Internet". Στην αριστερή περιοχή του παραθύρου που εμφανίζεται, κάνουμε κλικ στην "Αλλαγή ρυθμίσεων προσαρμογέα". Στο νέο παράθυρο κάνουμε δεξί κλικ στην επιλογή "Τοπική σύνδεση" και στο μενού που αναδύεται επιλέγουμε τις "Ρυθμίσεις". Αν στο δικό σας σύστημα εμφανίζονται παραπάνω από μία "Τοπικές συνδεσεις", θα πρέπει να επιλέξετε εκείνη που αντιστοιχεί στην κάρτα δικτύου στην οποία έχετε συνδέσει το AP121U. Στο παράθυρο που ανοίγει, εντοπίζουμε το "Πρωτόκολλο Internet Έκδοση 4 (TCP/IPv4)" και κάνουμε πάνω του διπλό κλικ. Στο νέο παράθυρο (Σ.τ.Α: Έλεος, μ' αυτά τα Windows!) επιλέγουμε τη "Χρήση της παρακάτω διεύθυνσης IP", θέτουμε τη στατική διεύθυνση "192.168.2.11" και πατάμε OK προκειμένου ν' αποθηκευτούν οι ρυθμίσεις μας.

Αφού ξεμπερδέψουμε με τη ρύθμιση της κάρτας δικτύου, προχωράμε στη ρύθμιση της σειριακής θύρας. Κατ' αρχάς, συνδέουμε τον μετατροπέα USB σε TLL-UART στον υπολογιστή, ώστε να εγκατασταθούν από το σύστημα οι απαιτούμενοι drivers. Αν δεν βρεθούν οι κατάλληλοι drivers αυτόματα (το πιο πιθανό :P) πρέπει να τους αναζητήσουμε μόνοι μας στο Internet. Πάντως, αν έχετε ακολουθήσει την προτροπή μας κι έχετε προμηθευτεί μετατροπέα με το τσιπάκι CP2102, μπορείτε να κατεβάσετε τον driver από το https://app.box.com/shared/i3qahx4z3k9a8xa1260g. Μετά την εγκατάσταση ανοίγουμε πάλι τον Πίνακα Ελέγχου. Αυτή τη φορά κάνουμε κλικ στο "Σύστημα και Ασφάλεια" κι αμέσως μετά στο "Σύστημα". Από το μενού στην αριστερή περιοχή του παραθύρου επιλέγουμε τη "Διαχείριση Συσκευών". Στο νέο παράθυρο, εντοπίζουμε τη σειριακή θύρα (COM Port) που προστέθηκε στο σύστημα, όταν εγκαταστήσαμε τον driver του αντάπτορα. Κάνουμε δεξί κλικ επάνω στη θύρα κι

επιλέγουμε τις ρυθμίσεις. Στο νέο-νέο παράθυρο (υπομονή, παιδία!) επιλέγουμε την καρτέλα "Ρυθμίσεις θυρών" κι από εκεί πραγματοποιούμε τις ακόλουθες ρυθμίσεις:

- Bit ανά δευτερόλεπτο / Bits per second ή Baud rate: 115200
- Bit δεδομένων / Data bits: 8
- Ισοτιμία / Parity: None
- Bit διακοπής / Stop bits: 1
- Έλεγχος ροής / Flow control: None

Όταν τελειώσουμε με τη ρύθμιση της σειριακής θύρας, εγκαθιστούμε τα προγράμματα που αναφέραμε νωρίτερα (TFTP server, WinSCP και putty). Τέλος, κατεβάζουμε τα απαραίτητα πακέτα με το firmware και τα τοποθετούμε σε κάποια πρόχειρη αλλά ευπρόσιτη τοποθεσία.



Η επιτυχία "ζωγραφισμένη" σε ένα τερματικό. Έχουμε συνδεθεί στη συσκευή μέσω SSH και, όπως βλέπετε, το σύστημα αυτοχαρακτηρίζεται ως "WiFi Pineapple Mark IV" και μας υποδέχεται μ' ένα όμορφο ASCII art.

Εκκίνηση διαδικασίας

Σε αυτό το στάδιο το ρουτεράκι συνδέεται με τον υπολογιστή μέσα από δύο διαφορετικές "διαδρομές": Διαμέσου του μετατροπέα USB σε TTL-UART και μέσω του καλωδίου Ethernet. Τώρα πρέπει να ανοίξουμε ένα το PuTTY, για να προετοιμάσουμε τη σύνδεση των συσκευών μέσω σειριακής θύρας. Στο αριστερό τμήμα του παραθύρου του προγράμματος, κάνουμε κλικ στο Serial (τελευταία επιλογή). Στο πρώτο πεδίο για συμπλήρωση εισάγουμε τη σειριακή θύρα που δημιουργήθηκε κατά τη σύνδεση του αντάπτορα (στην περίπτωσή μας είναι η COM4). Ακριβώς από κάτω δίνουμε τις τιμές που δώσαμε και νωρίτερα, για τη ρύθμιση της σειριακής θύρας. Κατόπιν, πάλι

από την αριστερή περιοχή του παραθύρου του προγράμματος, κάνουμε κλικ στην επιλογή Session. Στη δεξιά περιοχή του παραθύρου επιλέγουμε σαν "Connection type" το Serial και θέτουμε σαν Serial Line την COM4[2]. Στο πεδίο Speed δίνουμε το 115200 και πατάμε το κουμπί Open.

Στη παρούσα φάση το PuTTY θα εμφανίσει ένα κενό μαύρο παράθυρο και θα περιμένει στωικά, μέχρι να επικοινωνήσει κάποιος μαζί του. Σ' αυτό ακριβώς το στάδιο, μπορούμε να συνδέσουμε τη συσκευή μας στο ρεύμα. Μόλις ενεργοποιηθεί η συσκευή, θα επικοινωνήσει μέσω της σειριακής θύρας με τον υπολογιστή και στο παράθυρο του PuTTY θα εμφανιστούν μερικά μηνύματα από τον boot loader (U-boot). Πολύ σύντομα θα εμφανιστούν και τρεις επιλογές, από τις οποίες πρέπει να επιλέξουμε την πρώτη. Εδώ χρειάζεται προσοχή και λίγη ταχύτητα. Ο boot loader της συσκευής θα μας δώσει μόλις τρία δευτερόλεπτα για να ανταποκριθούμε. Η επιλογή που μας ενδιαφέρει (η πρώτη), θα μας εισαγάγει σε ένα περιβάλλον από το οποίο μπορούμε να εκτελέσουμε εντολές, πριν γίνει εκκίνηση του λειτουργικού.

Για να μπορέσουμε να προχωρήσουμε τώρα, πρέπει να ενεργοποιήσουμε τον TFTP Server. Στη δική μας περίπτωση τρέξαμε το πρόγραμμα tftpd32 και στο πεδίο "Current Directory" θέσαμε τον κατάλογο στον οποίο είχαμε αποθηκεύσει τα αρχεία του firmware. Ακριβώς από κάτω (Server Interfaces) επιλέξαμε την κάρτα δικτύου του υπολογιστή, στην οποία είχαμε συνδέσει τον υπό μετατροπή ρούτερ. Στη συνέχεια αφήσαμε τον TFTP server να τρέχει στο παρασκήνιο κι επιστρέψαμε στο PuTTY. Εκεί, εφόσον ο TFTP server λειτουργεί κανονικά και μοιράζει τα αρχεία με το firmware, πρέπει να εκτελέσουμε τις ακόλουθες εντολές:

```
setenv bootargs "board=ALFA console=ttyATH0,115200
rootfstype=squashfs,jffs2 noinitrd"
```

Η εντολή setenv προσθέτει ή τροποποιεί τις μεταβλητές του περιβάλλοντος του συστήματος. Εδώ δηλώνουμε μερικά απαραίτητα στοιχεία στη μεταβλητή bootargs.

```
saveenv
```

Η δε εντολή saveenv χρησιμοποιείται για να αποθηκευτούν μόνιμα όσες αλλαγές έχουμε κάνει σε μεταβλητές περιβάλλοντος του συστήματος.

```
tftp 0x80600000 kernel.bin
```

Με αυτή την εντολή το ρουτεράκι μας θα συνδεθεί στον υπολογιστή και θα κατεβάσει το αρχείο kernel.bin. Το εν λόγω αρχείο δεν θα τοποθετηθεί σε κάποιο μόνιμο αποθηκευτικό μέσο, αλλά σε μία διεύθυνση της μνήμης (0x80600000). Μπορούμε να τσεκάρουμε πότε ολοκληρώθηκε η μεταφορά, από το σχετικό μήνυμα που θα εμφανίσει το tftpd32 στον υπολογιστή.

```
erase 0x9f650000 +0x190000
```

Με την εκτέλεση του παραπάνω, διαγράφουμε την υπάρχουσα εκδοχή του πυρήνα από τη μνήμη.

```
cp.b 0x80600000 0x9f650000 d695a
```

Εδώ πραγματοποιείται μια αντιγραφή του πυρήνα που μεταφορτώσαμε από τον υπολογιστή, στη θέση μνήμης όπου βρισκόταν ο εργοστασιακός. Επί της ουσίας, με τα τρία προηγούμενα βήματα καταφέραμε να αντικαταστήσουμε τον παλιό πυρήνα της συσκευής με αυτόν του OpenWRT. Με τον ίδιο τρόπο θα ανανεώσουμε και το σύνολο

2. Φυσικά, εσείς θα δηλώσετε τη σειριακή θύρα που δημιουργήθηκε στο δικό σας σύστημα κατά τη σύνδεση του αντάπτορα.

των αρχείων του συστήματος. Για το σκοπό αυτό, θα χρειαστεί να εκτελέσουμε τα ακόλουθα:

```
tftp 0x80600000 rootfs.bin
erase 0x9f050000 +0x600000
cp.b 0x80600000 0x9f050000 23d004
```

Σε αυτό το σημείο έχουμε εγκαταστήσει στο ρουτεράκι μας το OpenWRT. Τώρα πρέπει να εκτελέσουμε το νέο πυρήνα και στη συνέχεια να πραγματοποιήσουμε μια επανεκκίνηση:

```
bootm 0x9f650000
reboot
```

Όταν ολοκληρωθεί η επανεκκίνηση του συστήματος του ρούτερ και αφού σταματήσουν τα απανωτά μηνύματα στο PuTTY, πατάμε το πλήκτρο ENTER. Τώρα βρισκόμαστε πλέον στο κέλυφος του OpenWRT. Το πρώτο στάδιο της εγκατάστασης ολοκληρώθηκε με επιτυχία! Σειρά έχει η αλλαγή του password για το χρήστη root και η εκκίνηση του SSH server. Για την πρώτη εργασία χρησιμοποιούμε το προγραμματάκι passwd (το εκτελούμε χωρίς παραμέτρους και εισάγουμε το επιθυμητό συνθηματικό για το χρήστη root). Για την εκκίνηση του SSH server, αρκεί να δώσουμε κάτι τέτοιο:

```
/etc/init.d/dropbear start
```

Μετά την επιτυχημένη εκκίνηση του dropbear SSH server, μπορούμε να συνδεθούμε στο ρουτεράκι μας με δύο νέους τρόπους: Είτε με μια κρυπτογραφημένη συνεδρία τύπου SSH, είτε με το WinSCP στα Windows και το scp στο Linux, για την αντιγραφή αρχείων. Εμείς βεβαίως πρέπει να κάνουμε το δεύτερο, για να μεταφέρουμε στη συσκευή το firmware (upgrade.bin) του ανανά! Στη δική μας περίπτωση, λοιπόν, αφού ανοίξαμε το WinSCP, εφαρμόσαμε τις ακόλουθες ρυθμίσεις:

```
File Protocol: SCP
Host Name: 192.168.2.1
Port: 22
UserName: root
Password: το νέο κωδικό που ορίσαμε
```

Στη συνέχεια πατήσαμε το κουμπί Login και ξεκίνησε η σύνδεση με τη συσκευή. Όταν επιτεύχθηκε η σύνδεση, εμφανίστηκε ένα παράθυρο χωρισμένο σε δύο περιοχές: Στη μία εμφανίζονταν τα αρχεία του υπολογιστή και στην άλλη τα αρχεία του ρούτερ. Όπως αντιλαμβάνεστε, το περιβάλλον του WinSCP είναι εξαιρετικά εύχρηστο και επιτρέπει τις αντιγραφές με ένα απλό "drag and drop". Έτσι, αντιγράψαμε το αρχείο upgrade.bin (το firmware του Pineapple) στη θέση /tmp της συσκευής. Αν χρησιμοποιούσαμε Linux, θα μπορούσαμε να πετύχουμε το ίδιο αποτέλεσμα δίνοντας κάτι τέτοιο:

```
scp /path/to/upgrade.bin root@172.16.42.1:/tmp/
```

Σε κάθε περίπτωση, όταν μεταφέρουμε το firmware του Pineapple, επιστρέφουμε στη γραμμή εντολών της συσκευής και το εγκαθιστούμε:

```
sysupgrade -n -v /tmp/upgrade.bin
```

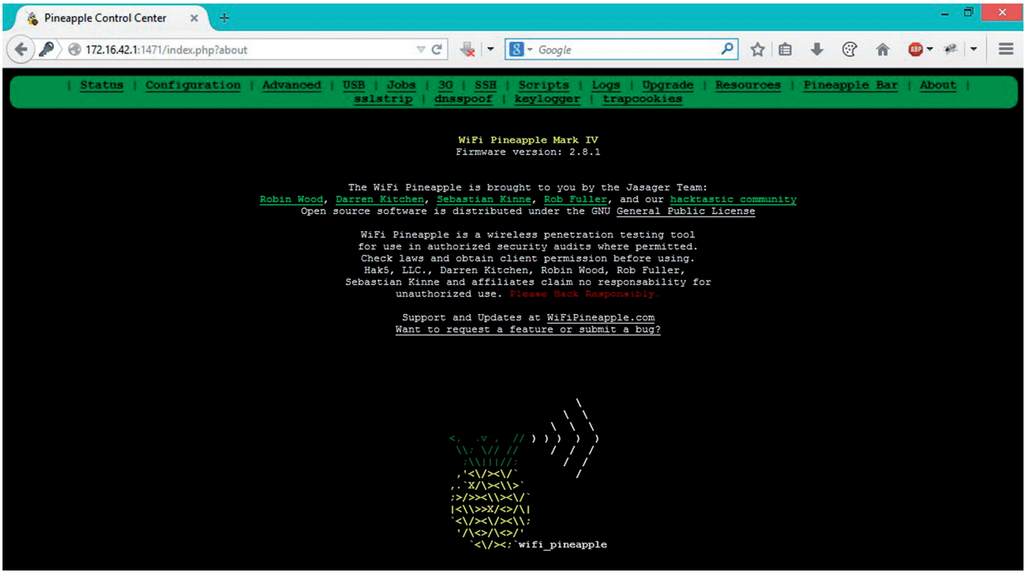
Μόλις ολοκληρωθεί κι αυτό το βήμα, είμαστε σχεδόν έτοιμοι. Αρκεί να κάνουμε να μια επανεκκίνηση και ο ανανάς μας θα είναι έτοιμος :D

Λίγη βαβούρα ακόμα

Εφόσον έχουν πάει όλα καλά, μπορούμε να συνδεθούμε στο web interface του Pineapple. Για να πετύχουμε κάτι τέτοιο, όμως, πρέπει να πραγματοποιήσουμε μια μικρή αλλαγή στις ρυθμίσεις του υπολογιστή μας. Εν συντομία, πρέπει να αλλάξουμε τη στατική διεύθυνση IP που ορίσαμε νωρίτερα στην κάρτα δικτύου του υπολογιστή. Για το σκοπό αυτό ακολουθούμε την ίδια διαδρομή (Πίνακας Ελέγχου → Δίκτυο και Internet → Συνδέσεις δικτύου), κάνουμε δεξί κλικ στη σύνδεση που αντιστοιχεί στη σωστή κάρτα δικτύου κι επιλέγουμε τις ρυθμίσεις. Στο νέο παράθυρο κάνουμε διπλό κλικ στο "Πρωτόκολλο Internet Έκδοση 4 (TCP/IPv4)" και στη συνέχεια αλλάζουμε τη στατική διεύθυνση που είχαμε δώσει σε "172.16.42.42". Αυτό ήταν όλο! Πατάμε το κουμπί ΟΚ για ν' αποθηκευτούν οι ρυθμίσεις μας και ανοίγουμε έναν browser. Για τη σύνδεση στο web interface του νέου μας ανανά, πρέπει να επισκεφθούμε τη διεύθυνση 172.16.42.1:1471. Για να εισέλθουμε στο web interface πρέπει να δώσουμε τα προκαθορισμένα στοιχεία σύνδεσης:

```
Username: root
Password: Pineapplesareyummy
```

Φυσικά, το πρώτο πράγμα που πρέπει να κάνουμε όταν συνδεθούμε, είναι να αλλάξουμε τον κωδικό πρόσβασης του root.



Το web interface του WiFi Pineapple μάς περιμένει στη διεύθυνση 172.16.42.1:1471. Από εκεί μπορούμε να ελέγξουμε όλες τις λειτουργίες της συσκευής και να τσεκάρουμε την κατάστασή τους.

Γεύση ανανά!

Μετά την ολοκλήρωση της διαδικασίας που περιγράψαμε, θα έχουμε ένα ολοκαίνουργιο, πάμφθηνο και πλήρως λειτουργικό WiFi Pineapple. Το WiFi Pineapple είναι μια εκπληκτική συσκευή με πάρα πολλές δυνατότητες. Αν θέλετε να μάθετε περισσότερα γι' αυτήν, μπορείτε να ανατρέξετε στο σχετικό άρθρο του τεύχους 005. Καλές δοκιμές και, όπως αναφέρει το ίδιο το Pineapple στη σελίδα About του web interface... Hack responsibly ;)

Skill: Intermediate
Tags: Setup, Installer, SFX, 7zip, WinRAR, IExpress

installer

by multiPetros

Οδηγοί εγκατάστασης [μέρος 1]

Οι οδηγοί εγκατάστασης είναι άρρηκτα συνδεδεμένοι με την εξελισσόμενη ευχρηστία των υπολογιστών και των προγραμμάτων. Μήπως όμως αυτές οι ευκολίες προορίζονται για προγράμματα που γράφτηκαν σε παλιότερες και πιο "παραδοσιακές" γλώσσες; Ε, λοιπόν, όχι! Εμείς θα επιμείνουμε στην Python και θα μάθουμε να ενσωματώνουμε οδηγούς εγκατάστασης σε όλα τα πνευματικά μας παιδιά.

Μέσα από το περιοδικό έχουμε προσεγγίσει πολλές φορές την ανάπτυξη προγραμμάτων με την αγαπημένη μας Python. Στο προηγούμενο τεύχος μάλιστα γνωρίσαμε έναν τρόπο ώστε τα scripts που γράφουμε σε Python να μετατρέπονται σε αυτοτελή εκτελέσιμα αρχεία. Αυτά τα αρχεία μπορούν να εκτελεστούν σε οποιοδήποτε σύστημα με Windows, ανεξάρτητα από το αν είναι παρών ο interpreter της Python ή όχι. Σ'αυτό το τεύχος θα ασχοληθούμε με τα συστήματα εγκατάστασης, τα οποία θα μας επιτρέψουν να αναπτύξουμε παντοδύναμους οδηγούς εγκατάστασης για την ακόμα ευκολότερη διανομή των προγραμμάτων μας.

Η αλήθεια είναι ότι οι οδηγοί εγκατάστασης απαντώνται πολύ συχνότερα (για να μην πούμε σχεδόν αποκλειστικά) στα Windows. Όπως αντιλαμβάνεστε, λοιπόν, η μελέτη μας θα περιοριστεί και πάλι στο λειτουργικό της Microsoft. Η λειτουργία των περισσοτέρων οδηγών εγκατάστασης συνοψίζεται ως εξής: Ο χρήστης, απαντώντας σε μια σειρά ερωτήσεων, τροφοδοτεί το σύστημα εγκατάστασης με τις απαραίτητες πληροφορίες για το ποια εξαρτήματα του προγράμματος πρέπει να εγκατασταθούν και σε ποια θέση πρέπει να τοποθετηθούν. Στη συνέχεια ο οδηγός μεταφέρει τα κατάλληλα αρχεία στις κατάλληλες θέσεις, δημιουργεί συντομεύσεις, προσθέτει το πρόγραμμα στη λίστα εφαρμογών του Πίνακα Ελέγχου και προετοιμάζει το πρόγραμμα απεγκατάστασης.

Οι διαθέσιμες επιλογές για τη δημιουργία οδηγών εγκατάστασης είναι πάρα πολλές. Εμείς θα ασχοληθούμε με εκείνες που είτε αποτελούν προϊόν Ελεύθερου Λογισμικού, είτε παρέχονται με μηδενικό κόστος. Σε κάθε περίπτωση, θα εξετάσουμε τις λύσεις που πιστεύουμε ότι έχουν το περισσότερο ενδιαφέρον. Φυσικά, η παρουσίασή μας θα ξεκινήσει από τις απλούστερες και ευκολότερες λύσεις, για να προχωρήσει στις πιο ισχυρές αλλά και απαιτητικές.

Δωράκι από τη Microsoft

Τα Windows, από την έκδοση 2000 κι έπειτα, έχουν κρυμμένο στα σπλάχνα τους ένα εργαλείο που πετυχαίνει αυτό που ζητάμε: Δημιουργεί συμπιεσμένα πακέτα που αποσυμπιέζονται κι εγκαθίστανται αυτόματα. Το εργαλείο αυτό ονομάζεται IExpress και κατοικεί στον κατάλογο /Windows/System32. Μάλιστα, επειδή ο συγκεκριμένος κατάλογος ανήκει εξ ορισμού στο λεγόμενο system path, μπορούμε να τρέξουμε το IExpress από οπουδήποτε δίνοντας, απλά, το όνομά του. Με άλλα λόγια, μπορούμε να ανοίξουμε το Start menu ή τη γραμμή εντολών και να δώσουμε ένα απλό "IExpress" (χωρίς τα εισαγωγικά). Το IExpress ενσωματώνει έναν ολόκληρο οδηγό, με τη βοήθεια του οποίου μπορούμε να κατασκευάσουμε άλλους οδηγούς :D Ας δούμε ποιες δυνατότητες προσφέρει το δωρεάν αυτό προγραμματάκι από τη Microsot.

Όταν το ξεκινάμε, μάς ρωτάει αν θέλουμε να δημιουργήσουμε ένα τέτοιο πακέτο από την αρχή ή να φορτώσουμε τις σχετικές παραμέτρους από κάποιο αρχείο (Self Extraction Directive file). Προφανώς, την πρώτη φορά που θα τρέξουμε το πρόγραμμα δεν θα έχουμε στη διάθεσή μας τέτοιο αρχείο ρυθμίσεων. Επομένως, θα πρέπει να επιλέξουμε το "Create new Self Extraction Directive file" και να προχωρήσουμε στο επόμενο βήμα. Εκεί παρέχονται τρεις επιλογές:

- Οδηγός εγκατάστασης που αποσυμπιέζει το περιεχόμενό του σ' έναν προσωρινό κατάλογο και κατόπιν εκτελεί κάποιο πρόγραμμα ή εντολή (εικόνα 1).
- Οδηγός εγκατάστασης που αποσυμπιέζει το περιεχόμενό του στην τοποθεσία που θα υποδείξει ο χρήστης.

- Οδηγός εγκατάστασης που δημιουργεί απλώς μια αρχειοθήκη CAB.

Όπως μάς ενημερώνει και το ίδιο το IExpress, η τρίτη επιλογή προορίζεται κυρίως για τη διανομή βιβλιοθηκών ActiveX (εικόνα 2). Η επιλογή που προσεγγίζει τις δικές μας ανάγκες περισσότερο από οποιαδήποτε άλλη είναι η δεύτερη.

Στο αμέσως επόμενο βήμα καθορίζουμε το όνομα του πακέτου εγκατάστασης. Ουσιαστικά, δηλώνουμε το όνομα που θα εμφανίζεται σαν τίτλος των διαφόρων παραθύρων του οδηγού εγκατάστασης (εικόνα 3). Στη συνέχεια έχουμε τη δυνατότητα να ορίσουμε το κείμενο για μια απλή ερώτηση προς το χρήστη. Πρακτικά, του ζητάμε μια επιβεβαίωση για το αν θέλουμε να πραγματοποιηθεί η εγκατάσταση ή όχι (εικόνα 4).

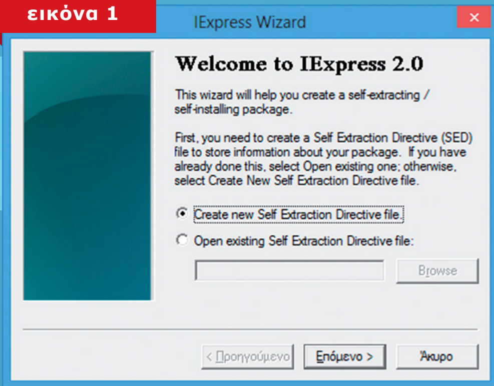
Τα προγράμματα διανέμονται συνήθως υπό τους όρους κάποιας άδειας χρήσης. Είναι σίγουρο ότι θα έχετε συναντήσει πολλές φορές το κουτάκι για το "διαβάσατε την άδεια χρήσης και συμφωνείτε", το οποίο θα πρέπει να τσεκάρετε υποχρεωτικά, αν θέλετε να πραγματοποιηθεί η εγκατάσταση. Είμαστε σίγουροι ότι οι περισσότεροι τσεκάρετε χωρίς να ρίξετε ούτε καν μια βιαστική ματιά στην άδεια :P Όπως και να 'χει, η εμφάνιση της άδειας χρήσης και η ερώτηση για την αποδοχή της από το χρήστη αποτελούν τυπικά βήματα στη διαδικασία εγκατάστασης ενός προγράμματος. Στο κάτω κάτω, οι περισσότεροι από εμάς είμαστε περήφανοι που δημιουργούμε και διανέμουμε προγράμματα υπό την άδεια GPL, οπότε γιατί να μην την εμφανίζουμε στους χρήστες μας; Το IExpress βοηθάει και σε αυτή τη δουλειά, επιτρέποντας να δηλώσουμε ένα αρχείο απλού κειμένου με την εκάστοτε άδεια χρήσης. Αργότερα, όταν θα εκτελέσουμε τον οδηγό που έχει δημιουργηθεί με το IExpress, θα εμφανιστεί η άδεια καθώς και η σχετική ερώτηση προς το χρήστη (εικόνα 5).

Στο επόμενο βήμα δηλώνουμε τα αρχεία που θέλουμε να περιλαμβάνονται στο πακέτο της εφαρμογής. Ένα σημαντικό μειονέκτημα εδώ είναι η αδυναμία εισαγωγής ολόκληρων καταλόγων. Το IExpress μάς υποχρεώνει να δηλώσουμε τα επιθυμητά αρχεία ένα προς ένα (εικόνα 6). Αμέσως μετά μπορούμε να επιλέξουμε τον τρόπο εμφάνισης του παραθύρου του οδηγού εγκατάστασης. Συγκεκριμένα, μπορούμε να επιλέξουμε αν θα πρόκειται για ένα κανονικό παράθυρο, αν θα είναι αόρατο, ελαχιστοποιημένο ή μεγιστοποιημένο (εικόνα 7).

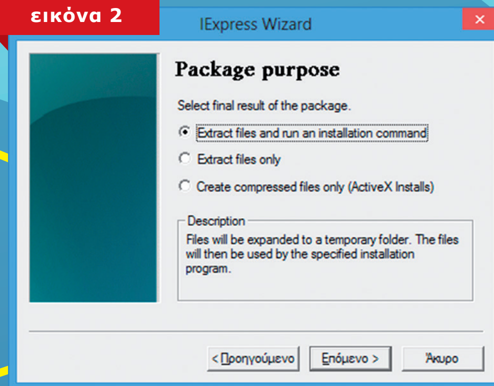
Μήπως θα θέλαμε να εμφανίζεται κάποιο μήνυμα όταν ολοκληρώνεται η εγκατάσταση που θα πραγματοποιεί ο οδηγός μας; Το IExpress παρέχει αυτή τη δυνατότητα και, φυσικά, ζητάει να του δώσουμε και το σχετικό μήνυμα (εικόνα 8). Ακολούθως καλούμαστε να επιλέξουμε το όνομα του οδηγού εγκατάστασης που θέλουμε να δημιουργηθεί και το αν θα εμφανίζει μπάρα προόδου στο χρήστη ή όχι (εικόνα 9). Τέλος, έχουμε τη δυνατότητα να αποθηκεύσουμε όλες τις επιλογές που έχουμε κάνει ως τώρα σε ένα αρχείο SED (Self Extraction Directive). Κάνοντας κάτι τέτοιο, αν αποφασίσουμε αργότερα να δημιουργήσουμε ένα νέο οδηγό εγκατάστασης για μια αναβαθμισμένη εκδοχή του προγράμματός μας, δεν θα χρειαστεί να επαναλάβουμε τη διαδικασία που είδαμε νωρίτερα. Αρκεί στο πρώτο βήμα να δώσουμε το συγκεκριμένο αρχείο SED κι ο οδηγός εγκατάστασης θα δημιουργηθεί αμέσως (εικόνα 10).

Μετά από όσα περιγράψαμε, η διαδικασία ολοκληρώνεται και το IExpress δημιουργεί τον οδηγό εγκατάστασης για το πρόγραμμά μας. Τα αποτελέσματα από τη χρήση του IExpress είναι σχετικά ικανοποιητικά, αφού δεν δημιουργεί συντομεύσεις ούτε κάποιο πρόγραμμα απεγκατάστασης, αλλά ικανοποιούν απόλυτα τις ανάγκες μας (βλ. εικόνες 11 έως 14).

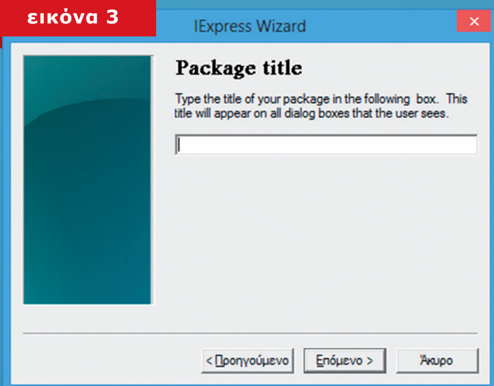
εικόνα 1



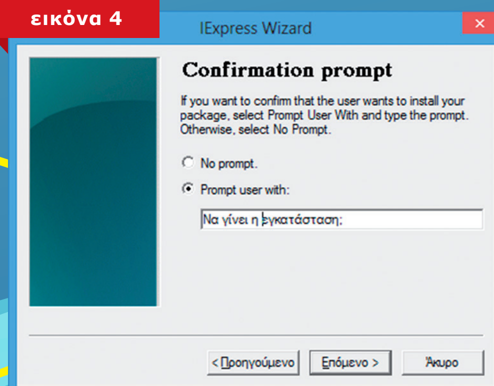
εικόνα 2



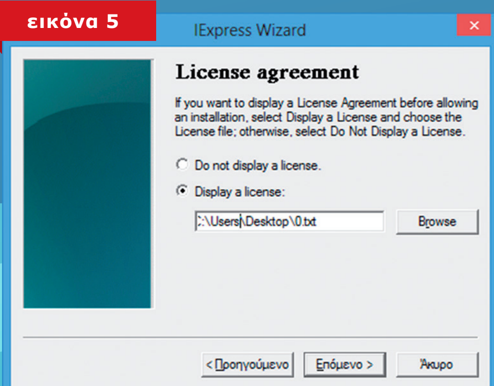
εικόνα 3



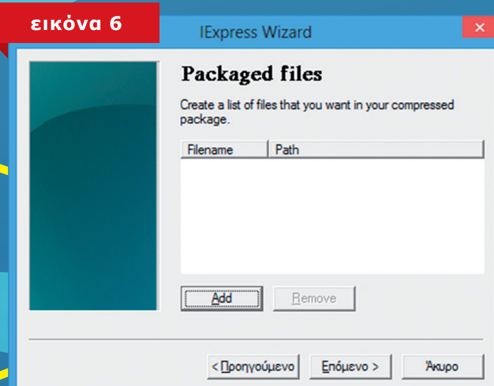
εικόνα 4



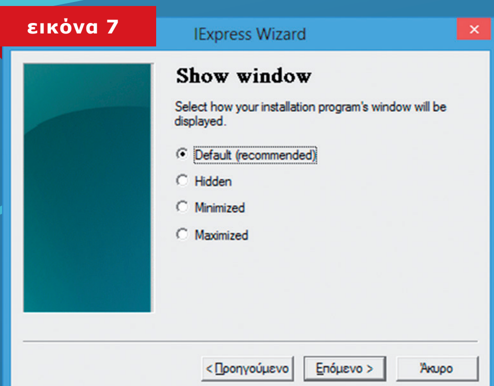
εικόνα 5

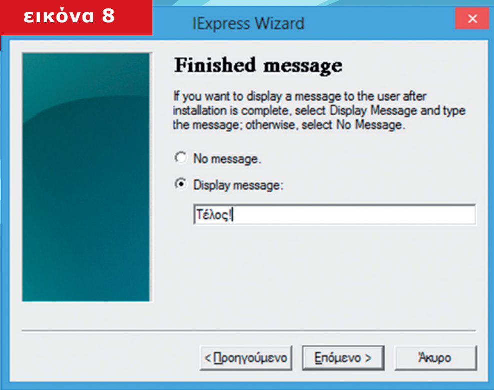


εικόνα 6

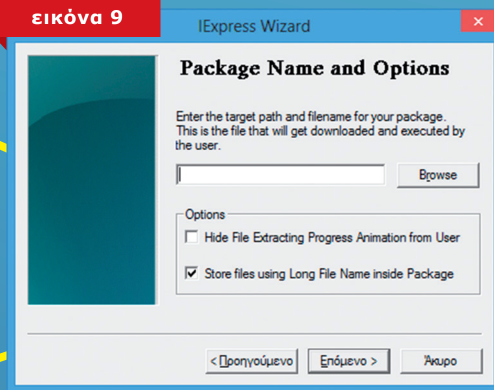


εικόνα 7

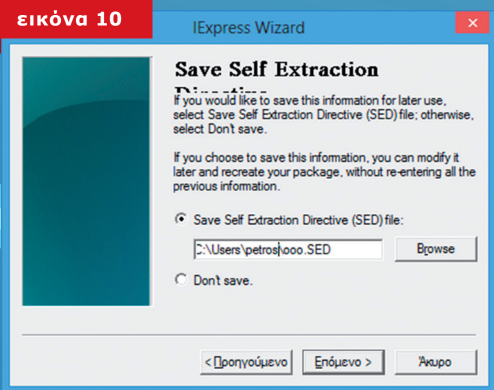




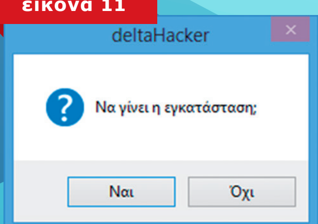
εικόνα 8



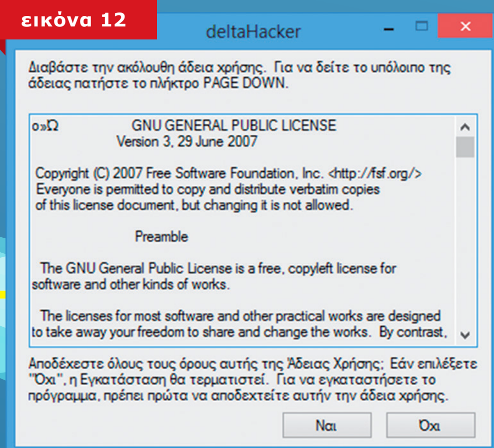
εικόνα 9



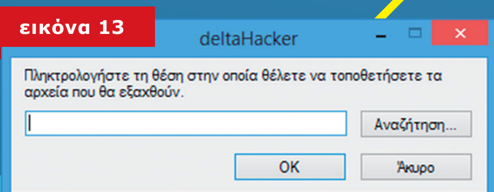
εικόνα 10



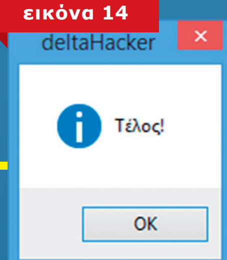
εικόνα 11



εικόνα 12



εικόνα 13



εικόνα 14

Οδηγοί αποσυμπίεσης

Μια άλλη λύση για την κατασκευή ενός απλοϊκού οδηγού εγκατάστασης, είναι η χρήση κάποιου από τα προγράμματα συμπίεσης κι αποσυμπίεσης. Τα περισσότερα από αυτά έχουν τη δυνατότητα να δημιουργούν συμπιεσμένα πακέτα, το οποία όμως είναι εκτελέσιμα και μπορούν να αποσυμπιέζονται από μόνα τους. Αναφερόμαστε στα λεγόμενα πακέτα SFX (Self Extract). Τα εκτελέσιμα του είδους δεν αποσυμπιέζουν το περιεχόμενό τους σε κάποια αυθαίρετη τοποθεσία, αλλά ρωτάνε το χρήστη. Σε ορισμένες περιπτώσεις τα εκτελέσιμα SFX μπορούν να επιτελέσουν κι άλλες λειτουργίες, όπως το άνοιγμα και την προβολή ενός αρχείου μετά την ολοκλήρωση της αποσυμπίεσης, την αυτόματη εκτέλεση κάποιου άλλου προγράμματος κ.λπ. Με λίγα λόγια, τα SFX συμπεριφέρονται σαν απλοί οδηγοί εγκατάστασης! Μερικά γνωστά εργαλεία που μπορούν να δημιουργήσουν πακέτα SFX είναι το αγαπημένο μας 7Zip και τα εμπορικά WinRAR και WinZip.

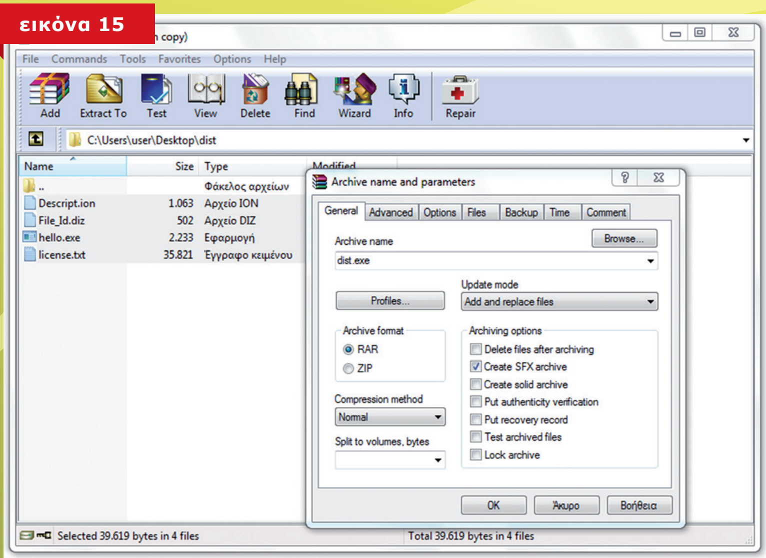
Προχωρημένες εγκαταστάσεις

Το 7Zip είναι εγκατεστημένο σε όλα τα μηχανήματα των εργαστηρίων της Parabing Creations (ανά τον κόσμο :D). Αυτά που μας έχουν κερδίσει είναι η υψηλή αποδοτικότητα του αλγορίθμου συμπίεσης που περιλαμβάνει, το γεγονός ότι μπορεί να χειριστεί συμπιεσμένα πακέτα οποιουδήποτε σχεδόν είδους, καθώς και το ότι αποτελεί προϊόν Ανοιχτού Λογισμικού. Το 7Zip δημιουργεί αρχεία SFX πανεύκολα, αλλά αυτά χαρακτηρίζονται από μια εξαιρετικά λιτή αισθητική κι ένα περιορισμένο σύνολο δυνατοτήτων. Έτσι, αν και πρόκειται για ένα από τα αγαπημένα μας εργαλεία, το 7Zip δεν αποτελεί την ιδανική επιλογή για την εργασία που μας ενδιαφέρει. Αντίθετα, το εμπορικό και κάπως βαρύ WinRAR έχει τη δυνατότητα να παράγει SFX με πολύ πιο πλούσια χαρακτηριστικά.

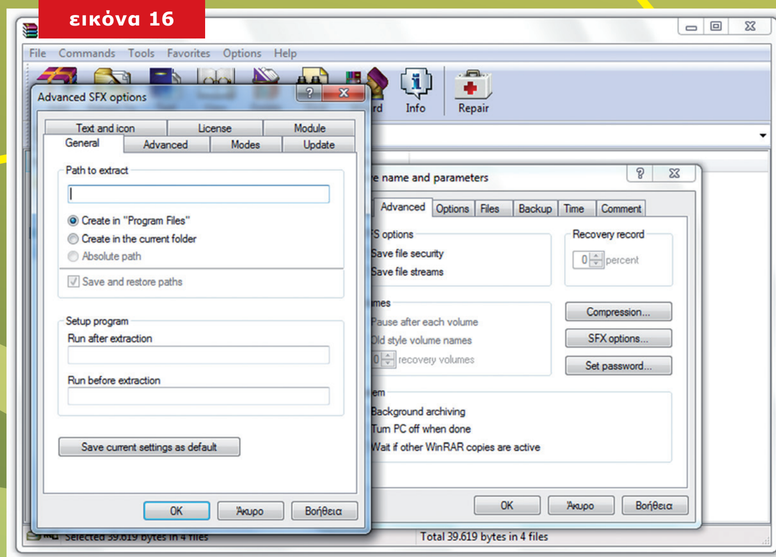
Για να δημιουργήσουμε ένα SFX με το WinRAR, πρέπει πρώτα να επιλέξουμε τα αρχεία που θα περιλαμβάνει το πακέτο μας μέσα από το περιβάλλον του προγράμματος και στη συνέχεια να πατήσουμε το κουμπί Add. Έτσι θα εμφανιστεί ένα νέο παράθυρο, στα δεξιά του οποίου υπάρχει η επιλογή "Create SFX Archive". Αν ενεργοποιήσουμε αυτή την επιλογή, εισάγουμε ένα όνομα στο πεδίο "Archive name" και πατήσουμε το κουμπί "OK", το WinRAR θα δημιουργήσει αμέσως το σχετικό πακέτο SFX. Με αυτόν τον τρόπο, όμως, οι λειτουργίες του πακέτου που παράγεται δεν διαφέρουν από εκείνες των πακέτων που δημιουργεί το 7Zip. Για να αποκτήσουμε πρόσβαση στις προχωρημένες λειτουργίες που προσφέρει το WinRAR, πάντα όσον αφορά στη δημιουργία πακέτων SFX, πρέπει να μεταβούμε στην καρτέλα Advanced και να πατήσουμε το κουμπί "SFX Options". Έτσι θα εμφανιστεί ένα νέο παράθυρο με τον τίτλο "Advanced SFX Options". Στις καρτέλες αυτού του παραθύρου θα βρούμε ένα πλούσιο σύνολο επιλογών για τη διαμόρφωση του υπό κατασκευή πακέτου SFX (εικόνα 15). Ας τους ρίξουμε μια ματιά.

Στην καρτέλα General, μπορούμε να καθορίσουμε την τοποθεσία στην οποία θα εξάγονται τα περιεχόμενα του πακέτου SFX. Επιπρόσθετα, μπορούμε να προσδιορίσουμε ένα πρόγραμμα που θέλουμε να εκτελεστεί πριν την αποσυμπίεση και κάποιο ακόμα που θα εκτελεστεί μετά (εικόνα 16).

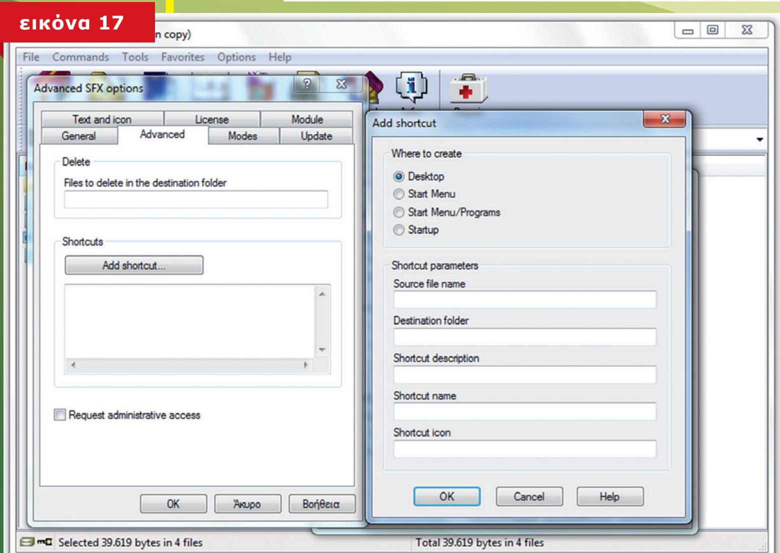
εικόνα 15



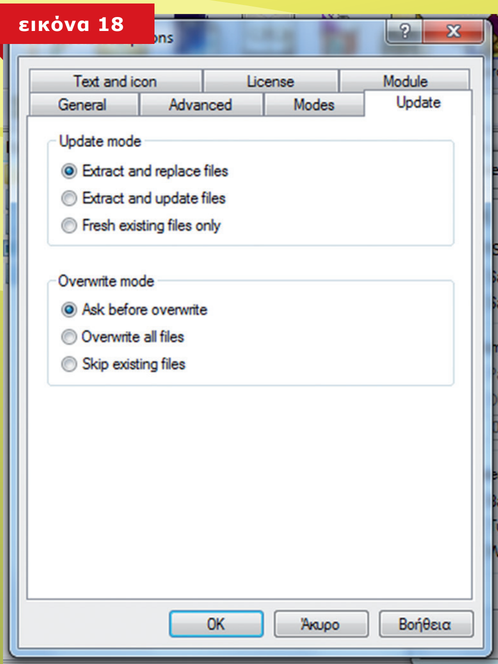
εικόνα 16



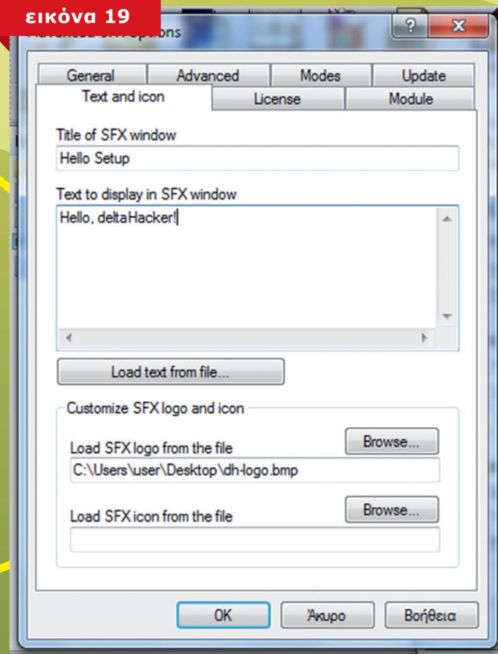
εικόνα 17



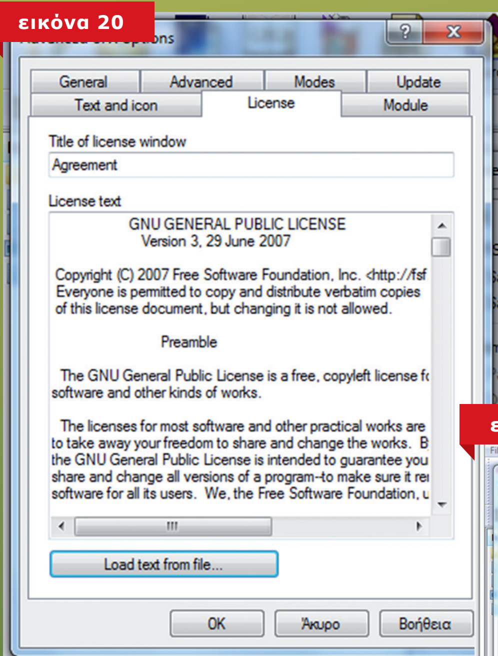
εικόνα 18



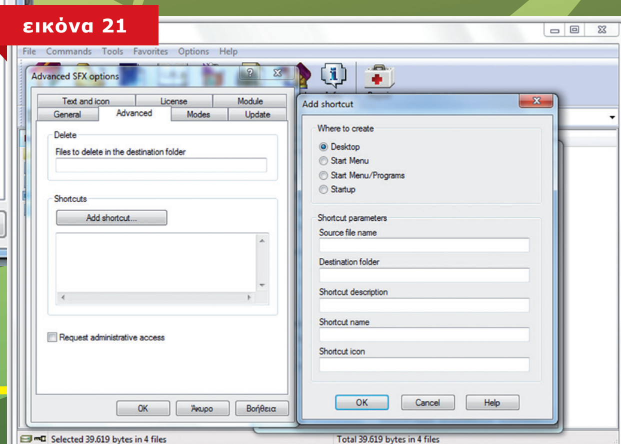
εικόνα 19



εικόνα 20



εικόνα 21



Από την καρτέλα Advanced μπορούμε να προσδιορίσουμε αρχεία που θα θέλαμε να διαγραφούν αυτόματα, όταν ολοκληρωθεί η αποσυμπίεση. Αυτή η λειτουργία μοιάζει περιττή, εφόσον δεν υπάρχει κανένας λόγος να προσθέσουμε άχρηστα αρχεία στο πακέτο. Ωστόσο, είναι πιθανό να προκύψουν άχρηστα αρχεία από την αυτόματη εκτέλεση των προγραμμάτων που ορίσαμε στην καρτέλα General. Το ξαναλέμε: είναι πιθανό, αλλά όχι σίγουρο. Εξάλλου, ενδέχεται να μην έχουμε επιβάλλει την εκτέλεση πρόσθετων προγραμμάτων. Όπως και να 'χει, οι επιλογές που προσφέρει το WinRAR προβλέπουν κάθε πιθανή περίπτωση! Στην ίδια καρτέλα (Advanced) και λίγο χαμηλότερα, υπάρχει το κουμπί "Add shortcut...". Πατώντας το εμφανίζεται ένα νέο παράθυρο, από το οποίο μπορούμε να καθορίσουμε τις παραμέτρους για τη δημιουργία μιας νέας συντόμευσης. Όπως αντιλαμβάνεστε, χρησιμοποιώντας το κουμπί "Add shortcut..." μπορούμε να ορίσουμε όλες τις συντομεύσεις που θέλουμε να δημιουργούνται αυτόματα από το πακέτο SFX (εικόνα 17).

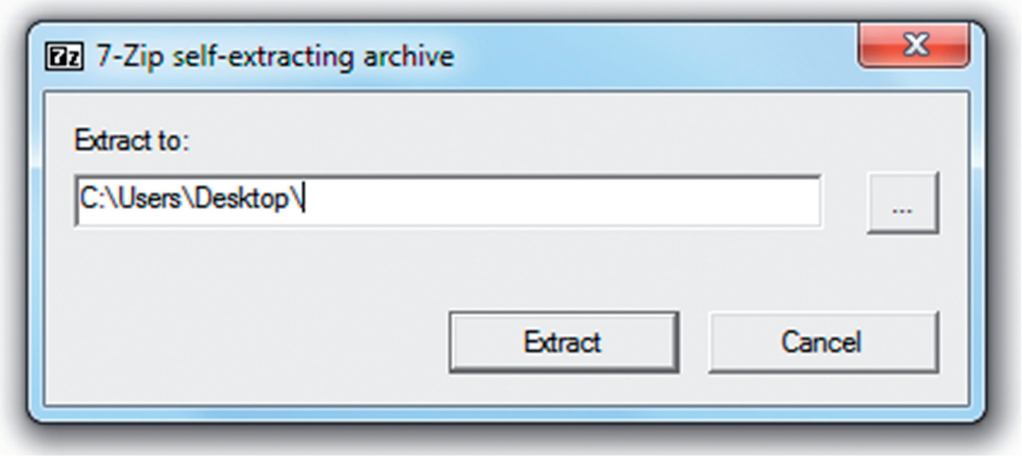
Τι θα συμβεί αν ο οδηγός εγκατάστασης που κατασκευάζουμε (εν προκειμένω το πακέτο SFX) προορίζεται για ένα update μιας ήδη υπάρχουσας εφαρμογής; Σε αυτή την περίπτωση, τα αρχεία του πακέτου πρέπει να αντικαταστήσουν εκείνα που θα βρεθούν στον κατάλογο προορισμού. Ή μήπως όχι; Το WinRAR προσφέρει αρκετές επιλογές για να προσδιορίσουμε επακριβώς τι θα συμβεί σε μία τέτοια περίπτωση και θα τις βρούμε όλες στην καρτέλα Update (εικόνα 18).

Περισσότερο ενδιαφέρον για την εργασία που εξετάζουμε παρουσιάζει η καρτέλα "Text and icon". Από εκεί μπορούμε να καθορίσουμε τον τίτλο που θα έχουν τα παράθυρα του πακέτου SFX, το "εισαγωγικό" κείμενο που θα εμφανίζεται στο χρήστη, το εικονίδιο του πακέτου SFX και το λογότυπο που θα εμφανίζει (εικόνα 19). Τέλος, για την ενσωμάτωση μιας άδειας χρήσης και τις σχετικές λειτουργίες προσφέρεται η καρτέλα License (εικόνα 20).

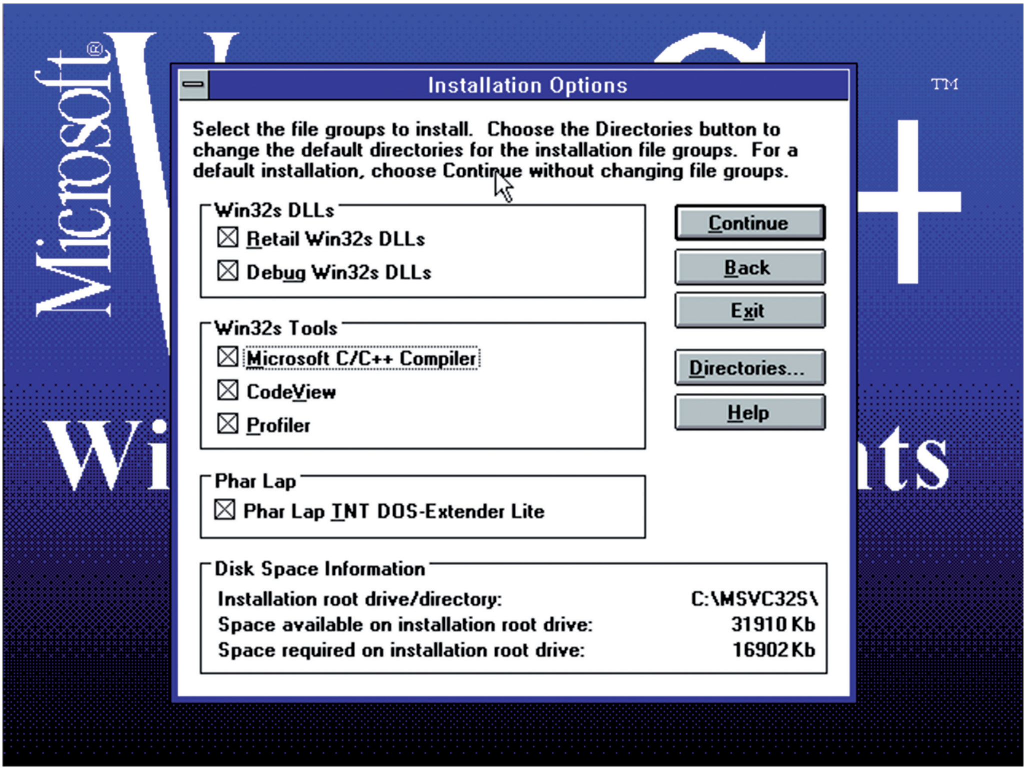
Αν και το WinRAR υπερτερεί ξεκάθαρα έναντι του IExpress, παρουσιάζει ένα μεγάλο μειονέκτημα: Δεν προβλέπει την αποθήκευση των ρυθμίσεων με *κανέναν* τρόπο. Επομένως, κάθε φορά που θέλουμε να δημιουργήσουμε ένα πακέτο SFX πρέπει να πραγματοποιούμε όλες τις ρυθμίσεις από την αρχή! Δεν πρέπει να μπερδευόμαστε, όμως. Το WinRAR δεν κατασκευάστηκε γι' αυτή τη δουλειά κι αποτελεί μόνο μια γρήγορη και πρόχειρη λύση (εικόνα 21).

Πέρασμα σε άλλη διάσταση

Οι λύσεις που παρουσιάσαμε μέχρι στιγμής είναι γρήγορες και εύκολες, αλλά δεν θα μπορούσαμε να τις χαρακτηρίσουμε επαγγελματικού επιπέδου. Αντιθέτως, θα τις χαρακτηρίζαμε ως ερασιτεχνικές. Στο επόμενο μέρος του άρθρου θα αφήσουμε πίσω αυτά τα "παιχνιδάκια" και θα εξετάσουμε μερικά εργαλεία δημιουργίας οδηγών εγκατάστασης, τα οποία χρησιμοποιούνται ακόμα και από τους κολοσσούς του Software! Ραντεβού στη σελίδα 42.



Τα πακέτα SFX που παράγει το 7Zip είναι εξαιρετικά λιτά και δεν προσφέρουν καμία ιδιαίτερη λειτουργία.



Οι οδηγοί εγκατάστασης στα Windows απαντώνται από τις πρώτες κιόλας εκδόσεις του λειτουργικού.

Skill: Beginner
Tags: Tor, torchat, tox, anonymity, privacy, encryption

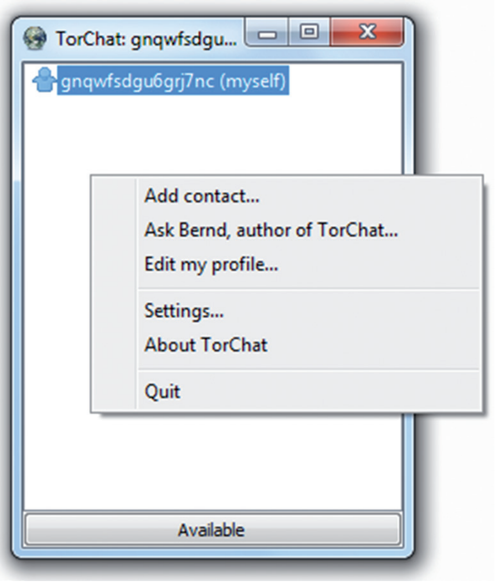


by multiPetros

TOX

Επικοινωνήστε άφοβα, μπορείτε!

Οι καθημερινές μας δραστηριότητες περιλαμβάνουν τη χρήση πολλών δικτυακών υπηρεσιών που παρέχονται δωρεάν. Μόνο που πίσω από το μηδενικό κόστος για την τσέπη μας, κρύβεται ένα μεγάλο κόστος για τη ιδιωτικότητά μας: Τα δεδομένα που ανταλλάσσουμε με άλλους χρήστες δεν ανήκουν πλέον σε εμάς, αλλά στις εταιρείες μέσω των οποίων πραγματοποιείται η επικοινωνία. Αν δεν μας πιστεύετε, διαβάστε τους όρους χρήσης. Αν πάλι μας πιστεύετε, συνεχίστε να διαβάζετε το άρθρο ;)

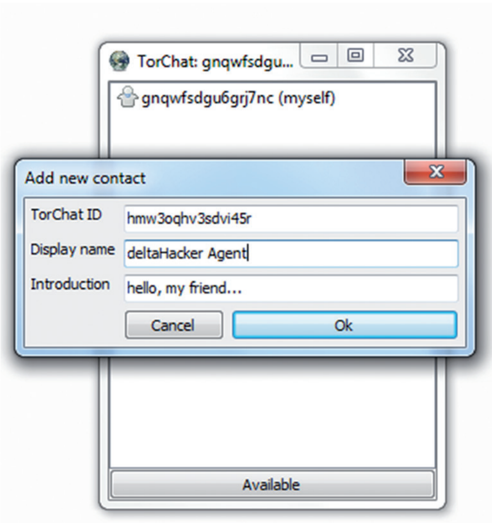


Το σπαρτιάτικο περιβάλλον του Torchat. Όλες οι παρεχόμενες λειτουργίες προσφέρονται από ένα μικρό pop-up menu, που εμφανίζεται με δεξί κλικ. Σημειώστε ότι το πρόγραμμα έχει γραφτεί σε Python και το περιβάλλον του σχηματίζεται με χρήση της βιβλιοθήκης wxPython.

Πριν από πολλά χρόνια, όταν το Internet είχε αρχίσει να εξαπλώνεται και να μπαίνει στα σπίτια μας με τις συνδέσεις dial-up, οι χρήστες αντάλλασσαν άμεσα μηνύματα μέσω IRC. Εκείνη την εποχή, όμως, το Internet δεν έπαιζε το ρόλο που παίζει σήμερα στην καθημερινή μας ζωή. Δεν πρέπει να μας προκαλεί αίσθηση, λοιπόν, ότι τότε ήταν ελάχιστοι εκείνοι που προβληματίζονταν για την ασφάλεια της επικοινωνίας τους. Με την πάροδο των χρόνων η χρήση του IRC περιορίστηκε και στη θέση του ξεφύτρωσαν διάφορες άλλες λύσεις. Ανάμεσα στους messengers που εμφανίστηκαν, ξεχωριστή παρουσία αποτελούσε το δημοφιλές Skype. Σε σχέση με τους προγόνους του παρείχε βελτιωμένες δυνατότητες επικοινωνίας, υποστηρίζοντας τόσο τη μεταφορά ήχου, όσο και εικόνας. Επιπρόσθετα, η αρχιτεκτονική του στηριζόταν σε τεχνολογία peer-to-peer (P2P), γεγονός που καθιστούσε δύσκολη την παρακολούθηση από τρίτους. Όπως θα γνωρίζετε, όμως, το Skype έχει περάσει πλέον στα χέρια της Microsoft. Μία από τις πρώτες αλλαγές που έκανε η εταιρεία-κολοσσός ήταν να μετατρέψει την αρχιτεκτονική του δικτύου από κατανεμημένη σε "συγκεντρωμένη" (centralized), επιβάλλοντας τη μεταφορά των μηνυμάτων μας από συγκεκριμένους κάθε φορά servers. Αυτό έγινε με πρόσχημα τη βελτίωση της ποιότητας των επικοινωνιών, αν και το αποτέλεσμα είναι αμφιλεγόμενο. Όπως και να 'χει, οι υποψιασμένοι χρήστες αντιμετωπίσαμε τη συγκεκριμένη αλλαγή με καχυποψία. Η καχυποψία μετατράπηκε σχεδόν σε βεβαιότητα, όταν αποκαλύφθηκαν οι πρακτικές της NSA και η συνεργασία της με διάφορες εταιρείες — μεταξύ των οποίων και η Microsoft.

Το Skype δεν αποτελεί το μοναδικό δημοφιλές δίκτυο για την πραγματοποίηση βιντεοκλήσεων. Υπάρχουν πολλές ακόμα λύσεις, αρκετές από τις οποίες προορίζονται για χρήση από smartphone. Οι συγκεκριμένες εφαρμογές προσφέρουν πολλές ευκολίες και το μόνο που ζητούν, συνήθως, είναι η πρόσβαση στον τηλεφωνικό μας κατάλογο. Μόνο που μ' αυτόν τον τρόπο οι αντίστοιχες εταιρείες μπορούν να συσχετίσουν τα ψευδώνυμά μας με τηλεφωνικούς αριθμούς κι άλλα πραγματικά στοιχεία, και κατά συνέπεια να ταυτοποιήσουν όχι μόνον εμάς τους ίδιους αλλά και τους συνομιλητές μας.

Για όσους ενδιαφέρονται για τη μυστικότητα της επικοινωνίας, έχουν αναπτυχθεί μερικές εξαιρετικές λύσεις οι οποίες μάλιστα είναι και Ανοιχτού Κώδικα. Πρόκειται για εφαρμογές ή και ολόκληρα δίκτυα, τα οποία προσφέρουν ασφάλεια κι ανωνυμία κρατώντας τα αδιάκριτα βλέμματα των εταιρειών και των κρατικών υπηρεσιών μακριά. Στο παρόν άρθρο θα παρουσιάσουμε δύο από τις πλέον ενδιαφέρουσες λύσεις: Το απλοϊκό torchat, του οποίου η λειτουργία θυμίζει τις πρώτες εκδόσεις του MSN Messenger, καθώς και το Tox, που παρέχει ένα πλούσιο οπλοστάσιο δυνατοτήτων και θα μπορούσε να συγκριθεί με το Skype!

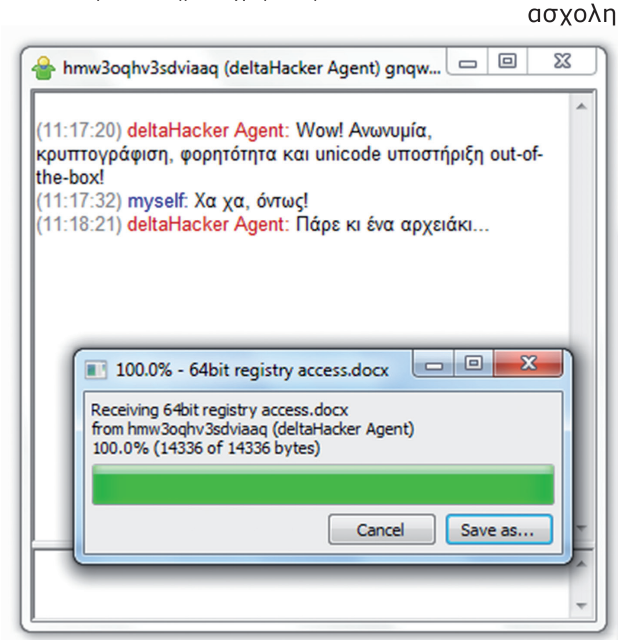


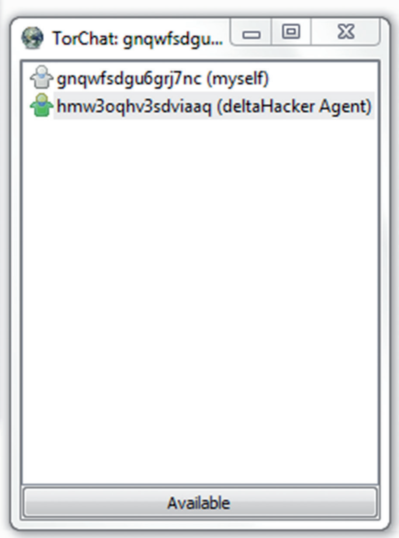
Η προσθήκη μιας επαφής στο Torchat είναι παιδικά απλή... νεύκολη. Το μόνο που πρέπει να γνωρίζουμε είναι το αντίστοιχο id. Κατά την προσθήκη της επαφής μπορούμε να ορίσουμε ένα ψευδώνυμο για την εύκολη διάκρισή της από τις υπόλοιπες, καθώς και ένα μήνυμα, που μπορείτε να το φαντάζεστε ως έναν αυτοματοποιημένο χαιρετισμό.

Ανωνυμία στο τσεπάκι μας

Το Torchat είναι ένας "σπαρτιάτικος" messenger, ο οποίος μεταφέρει μηνύματα κειμένου αλλά και αρχεία. Όπως φανερώνει το όνομά του, το Torchat αξιοποιεί το δίκτυο Tor προσφέροντας έτσι εγγυημένη ανωνυμία μεταξύ των συνομιλητών. Επιπρόσθετα, τα δεδομένα μας μεταφέρονται κρυπτογραφημένα. Χρησιμοποιώντας το Torchat είναι θεωρητικά αδύνατο να γνωρίζουμε ποιος μιλάει με ποιόν — εκτός φυσικά από τους ίδιους τους συνομιλητές! Το ίδιο ισχύει και για το περιεχόμενο των συνομιλιών, χάρη στην παρεχόμενη κρυπτογράφηση.

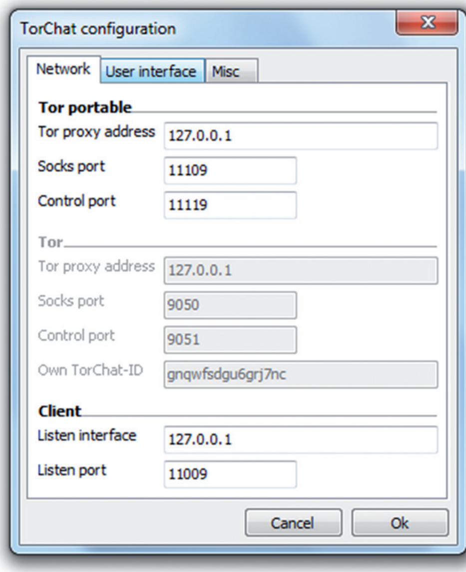
Το Torchat έχει αναπτυχθεί στην αγαπημένη μας Python κι ο πηγαίος του κώδικας διανέμεται υπό τους όρους της άδειας GNU GPL v3. Υπάρχουν εκδόσεις για Windows και για Linux, ενώ έχει αναπτυχθεί κι ένα παράγωγο έργο σε Java, υπό το όνομα jTorchat. Πάντως, για τις ανάγκες της παρουσίασης μας εμείς ασχοληθήκαμε με το "κλασικό " Torchat.





Η συνομιλία μέσω του Torchat χαρακτηρίζεται από αμεσότητα και κυρίως από απλότητα. Πάντως το πρόγραμμα υποστηρίζει την κωδικοποίηση unicode για τα μηνύματα, ενώ επιτρέπει και τη μεταφορά αρχείων.

Το πρόγραμμα παρέχεται με τη μορφή ενός πακέτου αρχείων και μπορούμε να το κατεβάσουμε από το https://github.com/prof7bit/TorChat/downloads. Το πακέτο περιλαμβάνει όλα τα απαραίτητα εξαρτήματα για τη σύνδεση στο δίκτυο ανωνυμίας του Tor και δεν απαιτεί από μέρους μας κάποια προεργασία (π.χ., την εγκατάσταση κάποιου άλλου εργαλείου). Έτσι, για να χρησιμοποιήσουμε το Torchat αρκεί να αποσυμπιέσουμε το πακέτο που κατεβάσαμε σε κάποιον κατάλογο και να τρέξουμε το εκτελέσιμο. Μιλάμε δηλαδή για ένα πρόγραμμα τύπου portable, με μέγεθος περί τα 10MB, που μπορεί να βρίσκεται στο flash drive που κουβαλάμε πάντα μαζί μας ;)



Στο παράθυρο ρυθμίσεων του Torchat συναντάμε τρεις καρτέλες, μέσω των οποίων μπορούμε να αλλάξουμε τον τρόπο διασύνδεσης του προγράμματος, όπως επίσης την εμφάνιση και τη συμπεριφορά του.

Κατά την πρώτη εκκίνηση του προγράμματος κι αφού επιτευχθεί η σύνδεση στο δίκτυο του Tor, ο χρήστης λαμβάνει ένα μοναδικό id: αυτό είναι το λεγόμενο onion address. Πρόκειται για το ισοδύναμο του ψευδωνύμου μας, βάσει του οποίου θα μπορεί κανείς να μας αναγνωρίσει και να μας μιλήσει. Όπως αντιλαμβάνεστε, ο τρόπος με τον οποίο θα γνωστοποιήσουμε στους φίλους μας το id είναι καθοριστικός για τη διασφάλιση της ανωνυμίας. Μια καλή ιδέα είναι η μετάδοση του id με ένα κρυπτογραφημένο (encrypted) και υπογεγραμμένο (signed) email. Κάνοντας δεξί κλικ στον κενό χώρο του κεντρικού παραθύρου του Torchat, μπορούμε να προσθέσουμε φίλους στη λίστα των επαφών μας. Στο παράθυρο που εμφανίζεται πρέπει να δώσουμε το id εκείνου με τον οποίο θέλουμε να επικοινωνήσουμε και, προαιρετικά, ένα ψευδώνυμο κι ένα μήνυμα που θα σταλεί αυτομάτως. Εδώ θα μπορούσαμε να δώσουμε ένα προσυνεννοημένο μήνυμα, με το οποίο ο συνομιλητής μας θα βεβαιωθεί για την ταυτότητά μας. Πάντως, μπορούμε κάλλιστα να αφήσουμε και το προεπιλεγμένο "hello my friend...". Στο ξεκίνημα της επικοινωνίας ενδέχεται να υπάρξει μια καθυστέρηση, η οποία όμως δεν πρέπει να μας ανησυχήσει καθόλου. Πρόκειται για μια φυσιολογική καθυστέρηση μέχρι να επιβεβαιωθεί η δυνατότητα σύνδεσης με την άλλη άκρη της γραμμής. Κατόπιν, μπορούμε να ξεκινήσουμε τη συνομιλία κανονικά και μάλιστα με υποστήριξη Unicode! Όπως είπαμε και αρχικά, εκτός από το κείμενο μπορούμε να στείλουμε και αρχεία. Αρκεί ένα δεξί κλικ στο εικονίδιο της αντίστοιχης επαφής ή μέσα στο παράθυρο συνομιλίας και η επιλογή του "Send file".

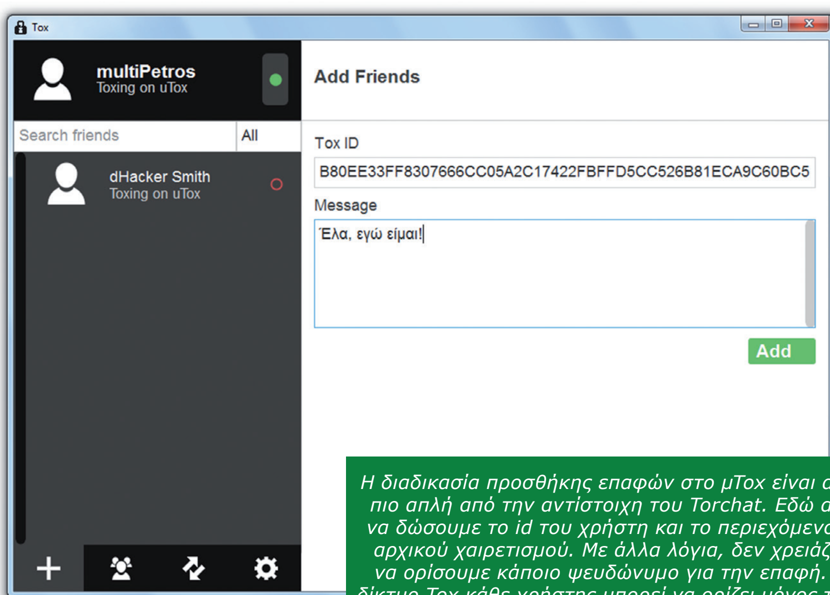
Να σημειώσουμε ότι, αν κλείσουμε το παράθυρο μιας συνομιλίας και στη συνέχεια το ανοίξουμε εκ νέου, θα μας περιμένει μια έκπληξη. Αν και θα περιμέναμε να δούμε τα μηνύματα που έχουμε ανταλλάξει με το συνομιλητή μας ως τώρα, θα αντικρύσουμε ένα κενό παράθυρο. Αυτό συμβαίνει γιατί οι εργοστασιακές ρυθμίσεις του προγράμματος δεν προβλέπουν την καταγραφή και την αποθήκευση των μηνυμάτων μας. Μάλιστα, αυτή η ρύθμιση αλλάζει ανά συνομιλητή. Έτσι, αν θέλουμε να ενεργοποιήσουμε την καταγραφή των μηνυμάτων που ανταλλάσσουμε με κάποιον, αρκεί να κάνουμε δεξί κλικ στο παράθυρο συνομιλίας με αυτόν τον "κάποιο" ή επάνω στην

αντίστοιχη επαφή και να επιλέξουμε το "Logging to file". Στη συνέχεια θα λάβουμε μια ειδοποίηση ότι η καταγραφή ενεργοποιήθηκε και την επόμενη φορά που θα κλείσουμε και θα ανοίξουμε το παράθυρο της συνομιλίας, θα μας περιμένουν όλα τα παλαιότερα μηνύματα.

Αν και το Torchat μπορεί να λειτουργήσει αμέσως και χωρίς κάποια ιδιαίτερη ρύθμιση —out of the box, που λέγαμε και στο χωριό—, επιτρέπει να επέμβουμε σε αρκετές λεπτομέρειες της λειτουργίας του. Με δεξί κλικ στο κεντρικό παράθυρο του προγράμματος κι επιλογή του "Settings", εμφανίζεται ένα νέο παράθυρο με τρεις καρτέλες. Από την πρώτη μπορούμε να τροποποιήσουμε τις ρυθμίσεις της διασύνδεσης με το δίκτυο Tor, στην περίπτωση που δεν θέλουμε να χρησιμοποιήσουμε κάποιον Tor proxy της επιλογής μας. Από τις άλλες δύο καρτέλες μπορούμε να επέμβουμε στην εμφάνιση και στον τρόπο αλληλεπίδρασης του προγράμματος μαζί μας. Για το τέλος αφήσαμε μια σημαντική λεπτομέρεια. Αν δεν θέλουμε οι ρυθμίσεις και τα αρχεία καταγραφής να τοποθετούνται στον ίδιο κατάλογο με το πρόγραμμα, θα πρέπει να σβήσουμε το αρχείο "portable.txt". Κάνοντας κάτι τέτοιο, το Torchat θα αποθηκεύει τις ρυθμίσεις και τις συνομιλίες μας στον κατάλογο %AppData%\torchat (στα Windows) ή στον ~/.torchat (στο Linux).

Το βαρύ πυροβολικό

Σε αντίθεση με το Torchat, το Tox αποτελεί ένα θηρίο της δικτυακής επικοινωνίας που υποστηρίζει μέχρι και την ομαδική συνομιλία με ήχο και εικόνα. Μάλιστα, στην ατζέντα της ομάδας ανάπτυξης του Tox βρίσκονται λειτουργίες όπως η αναφορά ανάγνωσης των μηνυμάτων, η ενημέρωση για την πληκτρολόγηση του συνομιλητή, η τηλεδιάσκεψη, ο απομακρυσμένος έλεγχος του desktop καθώς και το Push-to-Talk. Εν ολίγοις, ο βασικός στόχος των προγραμματιστών του Tox είναι η δημιουργία ενός προγράμματος σαν το Skype, με γνώμονα την ασφάλεια της επικοινωνίας. Η

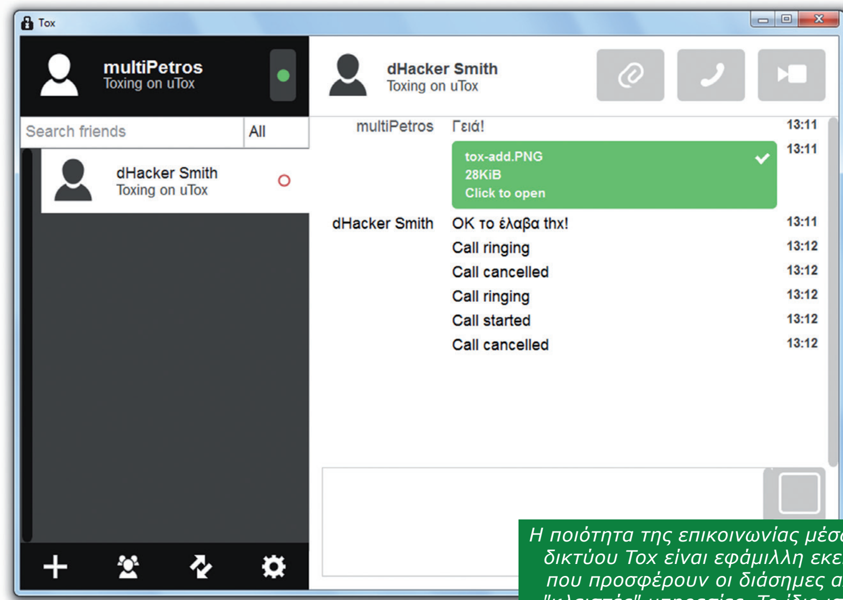


Η διαδικασία προσθήκης επαφών στο μTox είναι ακόμα πιο απλή από την αντίστοιχη του Torchat. Εδώ αρκεί να δώσουμε το id του χρήστη και το περιεχόμενο του αρχικού χαιρετισμού. Με άλλα λόγια, δεν χρειάζεται να ορίσουμε κάποιο ψευδώνυμο για την επαφή. Στο δίκτυο Tox κάθε χρήστης μπορεί να ορίζει μόνος του το προσωπικό του ψευδώνυμο.

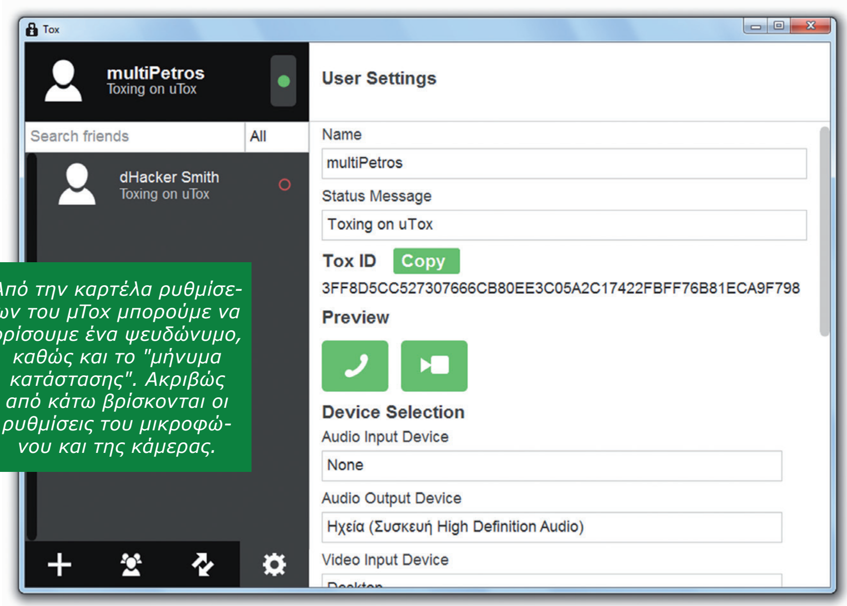
ανάπτυξη του Tox ξεκίνησε μόλις πριν ένα χρόνο, ενώ πολύ πρόσφατα (τον Αύγουστο!) προστέθηκαν οι δυνατότητες επικοινωνίας μέσω ήχου και βίντεο σε όλα τα προγράμματα-πελάτες του δικτύου του Tox. Και μιας και μιλήσαμε για δίκτυο, πρέπει να σας πούμε ότι το Tox βασίζει τη λειτουργία του σε ένα δίκτυο P2P, όπως και οι αρχικές εκδόσεις του Skype, δίχως τη χρήση κεντρικών servers. Μάλιστα, η όλη επικοινωνία μεταξύ των χρηστών πραγματοποιείται κρυπτογραφημένα, με τη χρήση ενός πρωτοκόλλου που αναπτύχθηκε ειδικά γι' αυτή τη δουλειά (Tox Protocol). Για τη διασφάλιση της ανωνυμίας, μιας και το Tox δεν χρησιμοποιεί το δίκτυο Tor, οι προγραμματιστές του έχουν υλοποιήσει μια τεχνική onion routing.

Όπως στο Torchat, έτσι και στο Tox ο εντοπισμός και η ταυτοποίηση των χρηστών δεν πραγματοποιείται με διευθύνσεις email, ούτε με ονόματα και τηλεφωνικούς αριθμούς. Χρησιμοποιούνται και πάλι ειδικά id, τα οποία όμως δεν αποτελούν διευθύνσεις εντός του δικτύου. Στην περίπτωση του Tox, το id ενός χρήστη σχηματίζεται από το αντίστοιχο δημόσιο κλειδί κρυπτογράφησης, σε συνδυασμό με μερικά ακόμα μεγέθη. Όλα αυτά μαζί συγκροτούν ένα μακροσκελές αναγνωριστικό με 76 δεκαεξαδικά ψηφία! Οι πρώτοι 64 χαρακτήρες αποτελούν το δημόσιο κλειδί του χρήστη, βάσει του οποίου κρυπτογραφούνται τα εισερχόμενα μηνύματα. Οι επόμενοι 8 χαρακτήρες αποτελούν μια τυχαία αλληλουχία, που χρησιμοποιείται για την αποφυγή των μηνυμάτων spam. Οποτεδήποτε θέλουμε να μπλοκάρουμε τα εισερχόμενα μηνύματα χωρίς να αλλάξουμε κλειδί κρυπτογράφησης, μπορούμε απλά να αλλάξουμε τους συγκεκριμένους οκτώ χαρακτήρες. Τα τελευταία 4 ψηφία του id αποτελούν δεδομένα που χρησιμοποιούνται από έναν αλγόριθμο ελέγχου της εγκυρότητας του id. Ουσιαστικά πρόκειται για το αποτέλεσμα της πράξης XOR μεταξύ του κλειδιού κρυπτογράφησης και των 8 ψηφίων που ακολουθούν.

Σ' αυτό το σημείο, οφείλουμε να κάνουμε μια διευκρίνιση: Το Tox δεν αποτελεί το



Η ποιότητα της επικοινωνίας μέσω του δικτύου Tox είναι εφάμιλλη εκείνης που προσφέρουν οι διάσημες αλλά "κλειστές" υπηρεσίες. Το ίδιο ισχύει και για την ευχρηστία!



Από την καρτέλα ρυθμίσεων του μTox μπορούμε να ορίσουμε ένα ψευδώνυμο, καθώς και το "μήνυμα κατάστασης". Ακριβώς από κάτω βρίσκονται οι ρυθμίσεις του μικροφώνου και της κάμερας.

όνομα ενός προγράμματος, αλλά το όνομα ενός δικτύου P2P, που βασίζεται στο Tox Protocol. Για κάθε πλατφόρμα υπάρχουν αρκετά προγράμματα-πελάτες (clients) που αξιοποιούν το εν λόγω δίκτυο. Φυσικά, μεταξύ όλων αυτών υπάρχουν και οι επίσημες υλοποιήσεις, που μπορούμε να βρούμε στη σελίδα `https://wiki.tox.im/Binaries`. Στον ακόλουθο πίνακα φαίνονται τα ονόματα "επίσημων" clients για καθένα από τα πιο δημοφιλή λειτουργικά συστήματα:

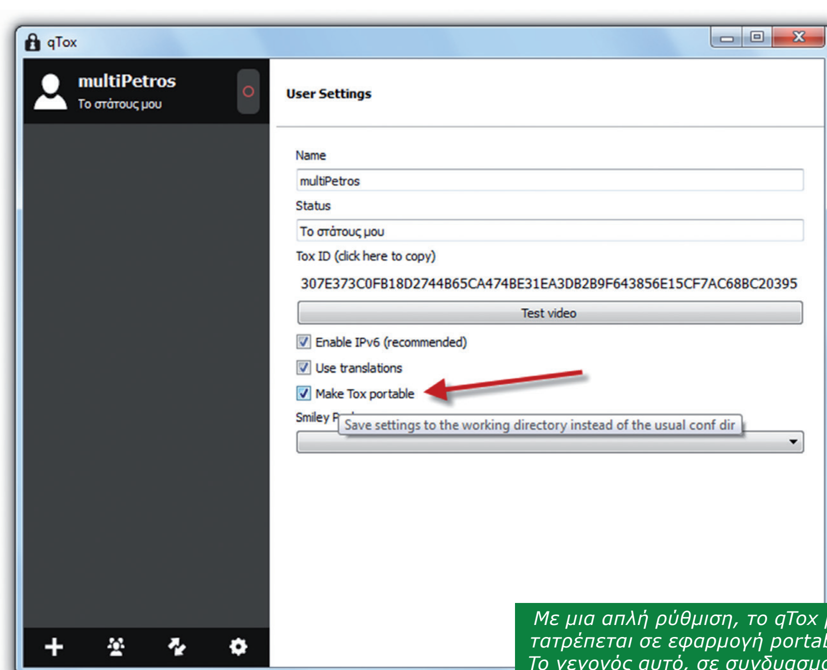
Σύστημα	Όνομα Client
MS Windows	μTox
Linux, FreeBSD	Venom
OSX	qTox
Android	Antox
iOS	Antidote

Η έκδοση του μTox για τα Windows, αν και δεν απαιτεί εγκατάσταση για τη λειτουργία της, δεν μπορεί να λειτουργήσει σαν τις τυπικές εφαρμογές portable. Αυτό συμβαίνει γιατί όλες οι ρυθμίσεις και τα κλειδιά κρυπτογράφησης αποθηκεύονται εξ ορισμού στον κατάλογο %AppData%\Tox. Όπως θα 'χετε καταλάβει, όμως, ο γράφων έχει μια μανία με τη φορητότητα. Έτσι, μετά από μια ενδελεχή αναζήτηση, εντοπίσαμε μια ικανοποιητικότατη και φορητή λύση. Πρόκειται για το πρόγραμμα qTox, το οποίο στηρίζεται στη γνωστή βιβλιοθήκη Qt. Η Qt διατίθεται, βεβαίως, για συστήματα Unix (Linux, FreeBSD, OSX, κ.ά.), αλλά προσφέρεται και για τα Windows. Παρεμπιπτόντως, εξαιτίας της ενσωμάτωσης της βιβλιοθήκης, το μέγεθός του qTox ανέρχεται στα 30MB και φαντάζει σαν ογκόλιθος μπροστά στα 1,7MB του μικροσκοπικού μTox. Πάντως το περιβάλλον των δύο προγραμμάτων είναι διευθετημένο με

παρόμοιο τρόπο, αν και το qTox ακολουθεί μια σαφώς "καθαρότερη" αισθητική. Από την περιοχή ρυθμίσεων του qTox μπορούμε να ενεργοποιήσουμε την αποθήκευση των ρυθμίσεων και των λοιπών δεδομένων στον κατάλογο όπου βρίσκεται η ίδια η εφαρμογή. Έτσι, ο κατάλογος με το πρόγραμμα μπορεί να τοποθετηθεί οπουδήποτε και στην πράξη η εφαρμογή γίνεται portable.

Αν τώρα οι δυνατότητες των Tox clients σας αφήνουν παγερά αδιάφορους και επιμένετε στη χρήση των Pidgin και Miranda, σας έχουμε ιδιαιτέρως ευχάριστα νέα. Υπάρχουν plugins και για τα δύο αυτά προγράμματα, που επιτρέπουν τη σύνδεση με το δίκτυο του Tox! Μάλιστα, για τους σκληροπυρηνικούς χρήστες της κονσόλας παρέχεται και ένας client που δεν απαιτεί παραθυρικό περιβάλλον. Πρόκειται για το πρόγραμμα Toxic, που παρέχεται για συστήματα Unix και, όπως αντιλαμβάνεστε, δεν (θα μπορούσε να) υποστηρίζει βιντεοκλήσεις.

Τέλος, κάτι ακόμα που αξίζει να αναφέρουμε είναι η δυνατότητα χρήσης του δικτύου Tox για "άσχετα" projects. Ένα απ' αυτά ακούει στο όνομα ToxBox και προβλέπει τη χρήση του δικτύου P2P του Tox για τον ασφαλή συγχρονισμό αρχείων. Κατά κάποιον τρόπο, αποτελεί μια αντιγραφή του δημοφιλούς —αλλά κλειστού κώδικα— Bittorent Sync. Για την ώρα, το ToxBox παραμένει στη σφαίρα του ιδεατού, αλλά δεν παύει να αποτελεί ένα πρώτης τάξεως δείγμα για τις δυνατότητες του δικτύου Tox.



Με μια απλή ρύθμιση, το qTox μετατρέπεται σε εφαρμογή portable. Το γεγονός αυτό, σε συνδυασμό με το αισθητικά "καθαρό" περιβάλλον, μας έκανε να τον αγαπήσουμε!

Skill: Intermediate
Tags: NSIS, makeNSISw, Zip2Exe, hm nis edit, Inno setup, Inno script studio, Pascal

installer

by multiPetros

Οδηγοί εγκατάστασης [μέρος 2]

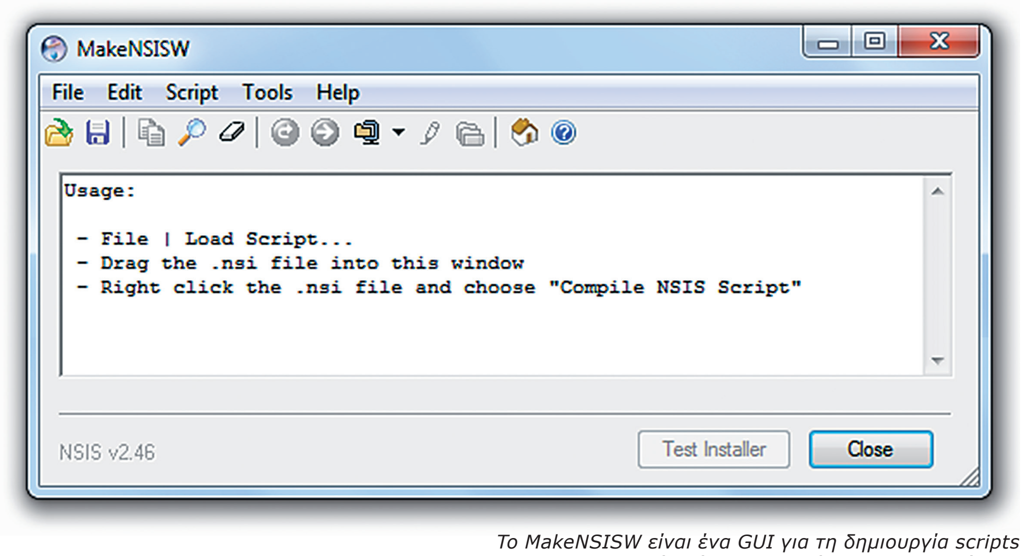
Συνεχίζουμε την περιήγησή μας στο χώρο των οδηγών εγκατάστασης, εξετάζοντας τα εξελιγμένα συστήματα NSIS και Inno Setup.

Η ανάγκη των developers να διευκολύνουν και σε τελική ανάλυση να ικανοποιήσουν τους χρήστες, είχε σαν συνέπεια τη δημιουργία των οδηγών εγκατάστασης. Η κατασκευή τέτοιων οδηγών από το μηδέν όμως εκτός από μπελαλίδικη, είναι και βαρετή. Έτσι, προέκυψαν εξειδικευμένα εργαλεία που αυτοματοποιούν τη σχετική εργασία και, επιπρόσθετα, παράγουν οδηγούς εγκατάστασης με πλούσιες δυνατότητες. Μερικές εταιρείες που εξειδικεύθηκαν στην ανάπτυξη τέτοιων εργαλείων είναι οι Flexera Software και Wise Solutions, οι οποίες δημιούργησαν τα συστήματα InstallShield, InstallAnywhere και Wise. Φυσικά, η κοινότητα των προγραμματιστών ανοιχτού κώδικα δεν θα μπορούσε να λείπει από το χορό. Εμείς, σ' αυτό το μέρος της περιπλάνησής μας, θα ασχοληθούμε με τα συστήματα εγκατάστασης ανοιχτού κώδικα και συγκεκριμένα θα εξετάσουμε τα NSIS και Inno Setup.

It really whips the Llama's ass![1]

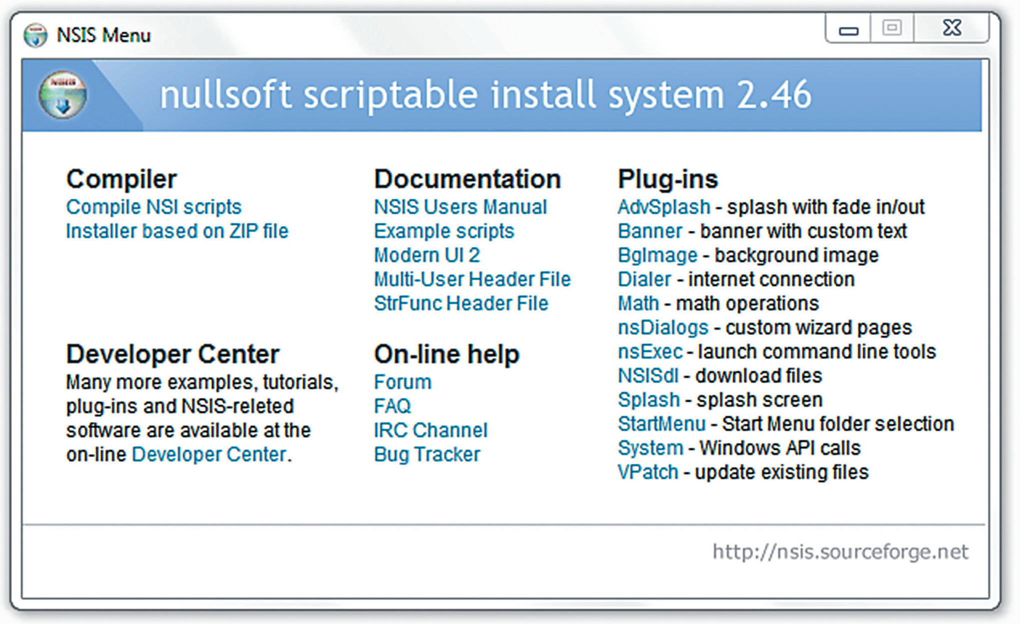
Το NSIS αποτελεί πνευματικό παιδί της Nullsoft, της εταιρείας που δημιούργησε το περίφημο Winamp και η οποία αργότερα εξαγοράστηκε από την AOL[2]. Το όνομα NSIS προέρχεται από τα αρχικά των λέξεων Nullsoft Scriptable Install System και αποκαλύπτει πολλά για τις ικανότητές του. Το NSIS αποτελεί προϊόν της εξέλιξης ενός συστήματος για το εύκολο πακετάρισμα των plug-ins του Winamp (PiMP, Plug-in Mini Packager) κι ο κώδικας του διανέμεται ελεύθερα.

Η παραγωγή των οδηγών εγκατάστασης —των τελικών εκτελέσιμων— πραγματοποιείται με τη βοήθεια του compiler του συστήματος NSIS, που ονομάζεται makeNSIS. Σε αυτόν δίνουμε ειδικά scripts, τα οποία περιγράφουν τις λειτουργίες του οδηγού εγκατάστασης που θέλουμε να δημιουργήσουμε. Μη σας ανησυχεί αυτό! Δεν είναι



Το MakeNSISW είναι ένα GUI για τη δημιουργία scripts του NSIS. Με τη βοήθειά του μπορούμε να συγκροτήσουμε εύχρηστους και ισχυρούς οδηγούς εγκατάστασης, αλλά θα πρέπει να γνωρίζουμε τη γλώσσα του NSIS!

1. Αυτό ήταν το slogan του WinAMP, με το οποίο μάς υποδεχόταν αμέσως μετά το πέρας της εγκατάστασής του. Για την ιστορία, να σημειώσουμε ότι προέκυψε από το τραγούδι "Whip The Llama's Ass" του Wesley Willis.
2. ...η οποία με τη σειρά της αποφάσισε τον τερματισμό της ανάπτυξης του WinAmp και ουσιαστικά το θάψιμό του :(



Το κεντρικό μενού του NSIS έχει κατά κύριο λόγο προπαγανδιστική λειτουργία! Διευκολύνει την εκμάθηση της γλώσσας του συστήματος, τόσο με παραδείγματα κώδικα όσο και με παραπομπές προς τα κείμενα της τεκμηρίωσης. Υπό μία έννοια προσπαθεί να μας μυήσει στον κόσμο του NSIS ;)

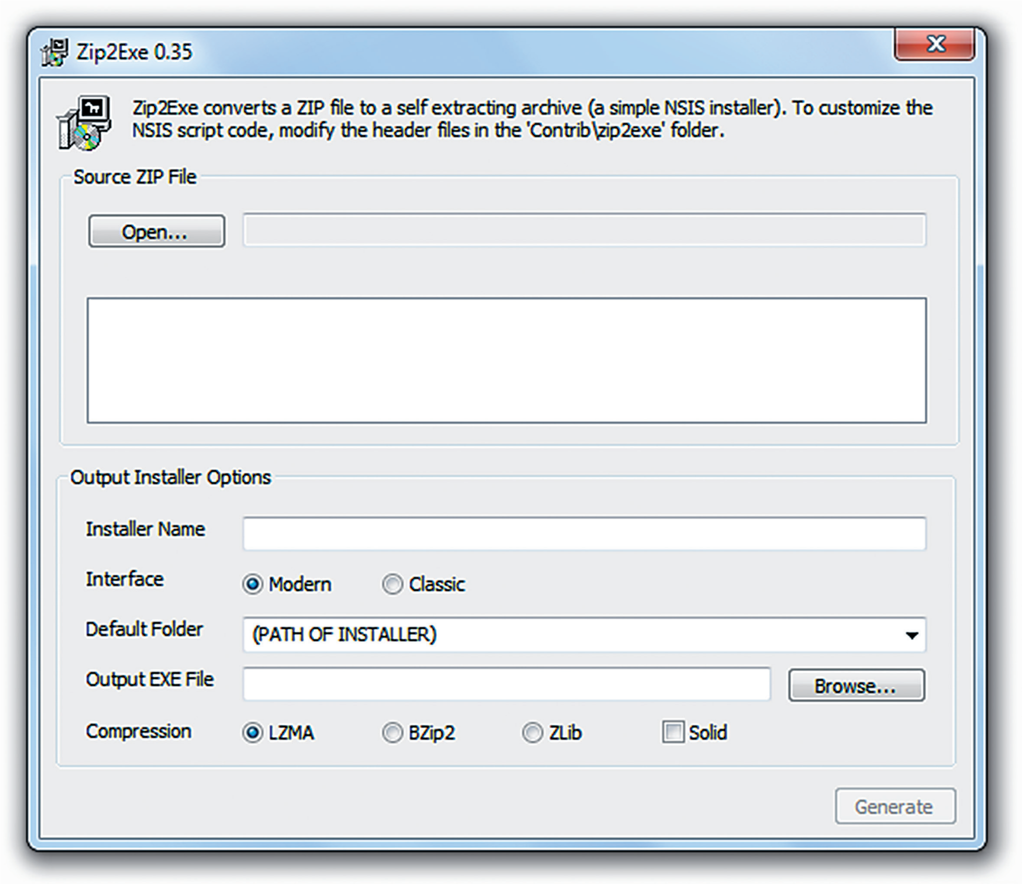
υποχρεωτικό να μάθετε μια ακόμα γλώσσα για scripting, αν δεν έχετε τη διάθεση. Υπάρχουν αρκετοί visual editors για το NSIS, με τη βοήθεια των οποίων μπορούμε να πετύχουμε εξαιρετικά αποτελέσματα. Ένας απ' αυτούς είναι ο HM NIS Edit, ο οποίος είναι και προϊόν ανοιχτού λογισμικού. Ας αφήσουμε τον πρόλογο, όμως, κι ας δούμε τη διαδικασία για την παραγωγή ενός οδηγού εγκατάστασης με το NSIS.

Ξεκινάμε μεταβαίνοντας στην τοποθεσία `http://NSIS.sourceforge.net`, απ' όπου μπορούμε να κατεβάσουμε την τελευταία έκδοση του NSIS. Αμέσως μετά περνάμε μια βόλτα κι από τη διεύθυνση `http://hmne.sourceforge.net`, στην οποία φιλοξενείται το HM NIS Edit . Όπως είπαμε ήδη, πρόκειται για το IDE που θα μας βοηθήσει στη δημιουργία ενός script για τον compiler του NSIS. Στη συνέχεια εγκαθιστούμε τα δύο προγράμματα — με τη σειρά που τα κατεβάσαμε.

Εργασία με το NSIS

Πριν ασχοληθούμε με το HM NIS Edit είναι καλό να γνωρίζουμε τις λειτουργίες που παρέχει το ίδιο το front-end του συστήματος NSIS. Ξεκινώντας το NSIS[3] εμφανίζεται ένα παράθυρο στο οποίο δεσπόζουν τρεις λίστες επιλογών. Αρχίζοντας από τα αριστερά συναντάμε τη λίστα με τίτλο Compiler, η οποία περιλαμβάνει τις επιλογές "Compile NSI Scripts" και "Installer based on ZIP file". Η πρώτη επιλογή ανοίγει το πρόγραμμα MakeNSISW, που αποτελεί ένα GUI για τον compiler ονόματι makeNSIS. Μέσα από αυτό το πρόγραμμα μπορούμε να γράψουμε τα δικά μας scripts ή ν' ανοι-

3. Εδώ αναφερόμαστε στο βασικό πρόγραμμα, στο front-end του συστήματος NSIS κι όχι σε ολόκληρο το σύστημα.



Δυστυχώς, η δημιουργία ενός αξιόλογου οδηγού εγκατάστασης απαιτεί κόπο. Εύκολος τρόπος δεν υπάρχει. Αυτό αποδεικνύει περίτρανα και η χρήση του απλοϊκού και πανεύκολου Zip2Exe.

ξουμε άλλα, που έχουμε ετοιμάσει ήδη. Παρεμπιπτόντως, τέτοιου είδους scripts δημιουργεί και το HM NIS Edit, που θα γνωρίσουμε σε λίγο. Η δεύτερη επιλογή ανοίγει το πρόγραμμα Zip2Exe. Το εν λόγω πρόγραμμα δημιουργεί οδηγούς εγκατάστασης που ενσωματώνουν τα περιεχόμενα ενός αρχείου Zip. Δηλαδή, το μόνο που έχουμε να κάνουμε είναι να υποδείξουμε στο πρόγραμμα ένα πακέτο Zip, να τσεκάρουμε τις λιγοστές ρυθμίσεις που παρέχει το πρόγραμμα και να πατήσουμε το κουμπί Generate. Με αυτόν τον τρόπο δημιουργούνται απλοϊκοί οδηγοί εγκατάστασης που ομοιάζουν μ' εκείνους του IExpress (δεν δημιουργούν συντομεύσεις, δεν προσθέτουν κάποια εγγραφή στη λίστα αφαίρεσης προγραμμάτων του Πίνακα Ελέγχου και δεν προσφέρουν πρόγραμμα απεγκατάστασης). Εμείς ωστόσο καταπιαστήκαμε με το NSIS γιατί ψάχνουμε κάτι πιο προχωρημένο και δεν θα περιοριστούμε στις απλοϊκές λύσεις που προσφέρει.

Ας επιστρέψουμε όμως στο παράθυρο με τις τρεις λίστες επιλογών. Η μεσαία περιλαμβάνει επιλογές για τη λήψη βοήθειας και την εκμάθηση της γλώσσας scripting του NSIS. Η λίστα στα δεξιά περιέχει παραδείγματα χρήσης των plug-ins που συνο-

δεύουν το NSIS. Επιλέγοντας κάποιο παράδειγμα ανοίγει ένα αρχείο απλού κειμένου, με την περιγραφή και τον κώδικα του παραδείγματος. Εν ολίγοις, θα λέγαμε ότι το front-end του NSIS επιτρέπει τη δημιουργία και τη μεταγλώττιση των δικών μας scripts, ενώ παράλληλα παρέχει την απαραίτητη τεκμηρίωση και διάφορα παραδείγματα για να μας βοηθήσει να μάθουμε τη γλώσσα του. Εμείς πάντως θα αφήσουμε την εκμάθηση της σχετικής γλώσσας σε όσους έχουν το μεράκι και θα εξετάσουμε μια ευκολότερη αλλά αρκετά αποτελεσματική λύση: Θα γνωρίσουμε το HM NIS Edit, που περιλαμβάνει έναν οδηγό για τη δημιουργία οδηγών εγκατάστασης[4].

Με την ευκολία του μαγικού ραβδιού

Το πρώτο πράγμα που βλέπει κανείς όταν ανοίγει το HM NIS Edit είναι ένα μεγάλο πλαίσιο κειμένου, έτοιμο να υποδεχτεί το script μας (εικόνα 1). Όπως όμως υποσχεθήκαμε, δεν σκοπεύουμε να καταπιαστούμε με τα scripts. Ρίχνοντας μια ματιά στη μπάρα εργαλείων του editor, διαπιστώνουμε ότι το δεύτερο κουμπί έχει το χαρακτηριστικό εικονίδιο ενός μαγικού ραβδιού: Όπως φαντάζεστε, πρόκειται για έναν οδηγό που θα δημιουργήσει το πολυπόθητο script, αφού μας απευθύνει μια σειρά ερωτήσεων και εμφανίσει όλες τις σχετικές επιλογές.

Το πρώτο βήμα του οδηγού είναι εισαγωγικό και δεν χρειάζεται να πούμε κάτι. Στο δεύτερο καλούμαστε να εισάγουμε τις βασικές πληροφορίες για την εγκατάσταση (εικόνα 2), όπως το όνομα της εφαρμογής μας, την έκδοσή της, το όνομα του προγραμματιστή (το δικό μας) και τη διεύθυνση της σχετικής ιστοσελίδας (αν υπάρχει). Στο επόμενο βήμα καλούμαστε να επιλέξουμε το εικονίδιο, το όνομα του οδηγού εγκατάστασης που θα δημιουργηθεί, τη γλώσσα του οδηγού εγκατάστασης, το είδος του περιβάλλοντος γραφικών του οδηγού, καθώς και τη μέθοδο συμπίεσης των αρχείων (εικόνα 3).

Στη συνέχεια ορίζουμε την προεπιλεγμένη (default) τοποθεσία εγκατάστασης, το αν θα έχει ο χρήστης να τροποποιήσει αυτή την τοποθεσία, καθώς και το κείμενο της άδειας χρήσης. Σε αυτό το σημείο μπορούμε να επιλέξουμε και τον τρόπο επιβεβαίωσης, για την αποδοχή της άδειας από το χρήστη (εικόνα 4). Αμέσως μετά καλούμαστε να συγκροτήσουμε μια λίστα με τα αρχεία που θα περιλαμβάνει και θα εγκαθιστά ο οδηγός μας. Εκτός από μεμονωμένα αρχεία, σε αυτή τη λίστα μπορούμε να εισάγουμε κι ολόκληρους φακέλους. Μάλιστα, για κάθε στοιχείο της λίστας μπορούμε να ορίσουμε την αντίστοιχη τοποθεσία εγκατάστασης! Επιπρόσθετα, για κάθε στοιχείο της λίστας μπορούμε να επιλέξουμε και το αν η εγκατάστασή του θα είναι προαιρετική ή όχι και κατ' επέκταση το αν θα ερωτάται ο χρήστης ή όχι (εικόνα 5).

Το επόμενο βήμα αφορά στη δημιουργία συντομεύσεων εντός του μενού Έναρξη των Windows. Από εδώ καθορίζουμε το όνομα του "φακέλου" που θα δημιουργηθεί μέσα στο μενού, αλλά μπορούμε και να επιτρέψουμε την αλλαγή του από το χρήστη. Επιπλέον είναι δυνατό να δημιουργήσουμε συντομεύσεις και για άλλα στοιχεία της εγκατάστασης, ενώ παρέχεται και η δυνατότητα προσθήκης μιας συντόμευσης για το πρόγραμμα απεγκατάστασης (εικόνα 6). Συνεχίζοντας τη διαδικασία, καλούμαστε να δηλώσουμε το κύριο εκτελέσιμο της εφαρμογής που θα εγκαθίσταται από τον οδηγό μας. Το συγκεκριμένο πρόγραμμα θα εκτελείται με το πέρας της εγκατάστασης, εκτός αν ο χρήστης έχει απενεργοποιήσει τη σχετική επιλογή του οδηγού. Στο ίδιο βήμα ορίζουμε και το κλασικό αρχείο readme, το οποίο θα μπορεί ο χρήστης να διαβάσει πατώντας ένα κουμπάκι στον οδηγό (εικόνα 7). Στο προτελευταίο βήμα

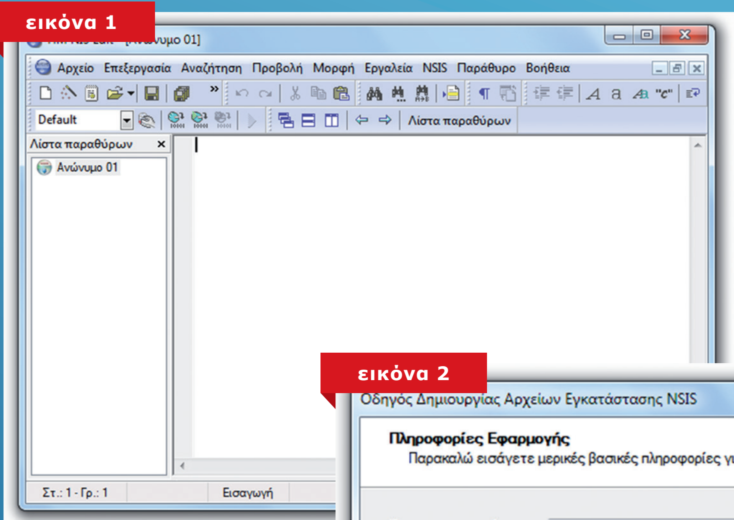
4. Υπάρχουν οδηγοί... μέχρι κάτω! Σας θυμίζει τίποτα αυτό; :D

έχουμε τη δυνατότητα τροποποίησης των βασικών μηνυμάτων που θα εμφανίζει το πρόγραμμα απεγκατάστασης (εικόνα 8).

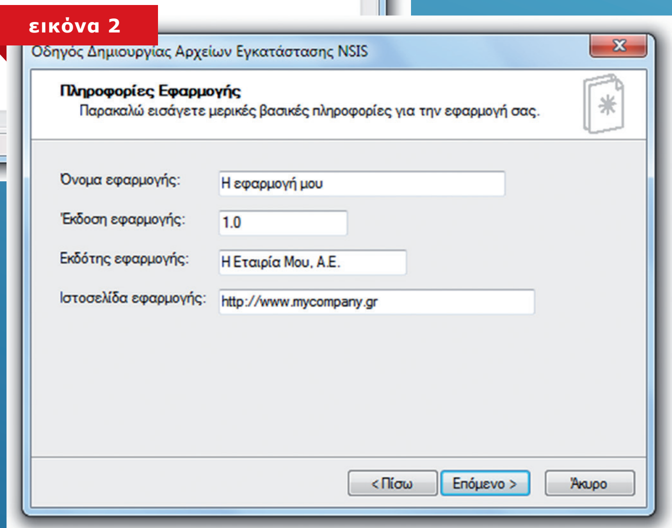
Πριν τερματίσουμε τον οδηγό του HM NSIS Edit, έχουμε τρεις επιλογές: Να αποθηκεύσουμε το script που θα δημιουργηθεί, να μετατρέψουμε τις διαδρομές των αρχείων από απόλυτες σε σχετικές ως προς τη θέση του script (κάτι ιδιαιτέρως χρήσιμο, αν σκοπεύουμε να μετακινήσουμε τα αρχεία της εφαρμογής μας) και, τέλος, να εκτελέσουμε μια μεταγλώττιση του script. Ουσιαστικά, η τελευταία επιλογή φορτώνει τον compiler του NSIS και τον τροφοδοτεί με το script που προκύπτει βάσει όλων των προηγούμενων βημάτων (εικόνα 9).

Αφού κλείσουμε τον οδηγό του HM NSIS Edit επιστρέφουμε στο κυρίως περιβάλλον εργασίας. Εκεί θα εμφανίζεται πλέον ο πηγαίος κώδικας του script που δημιουργήθηκε. Παρεμπιπτόντως, ακόμα και με μια γρήγορη ματιά, θα διαπιστώσετε ότι δεν είναι δυσνόητος καθώς κι ότι μπορείτε να κάνετε εύκολα επεμβάσεις και προσθήκες (εικόνα 10). Πάντως, μέσα από το HM NSIS Edit μπορούμε να πραγματοποιήσουμε ακόμα πιο προχωρημένες εργασίες, όπως η χειροκίνητη δημιουργία φορμών. Είμαστε πάντως σίγουροι ότι, όταν δείτε τους οδηγούς που παράγονται από το NSIS με τη βοήθεια του HM NSIS Edit, θα θελήσετε να εμβαθύνετε περισσότερο.

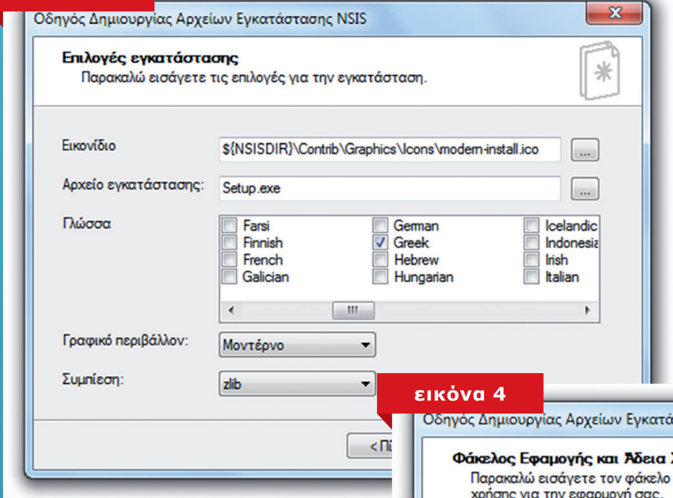
εικόνα 1



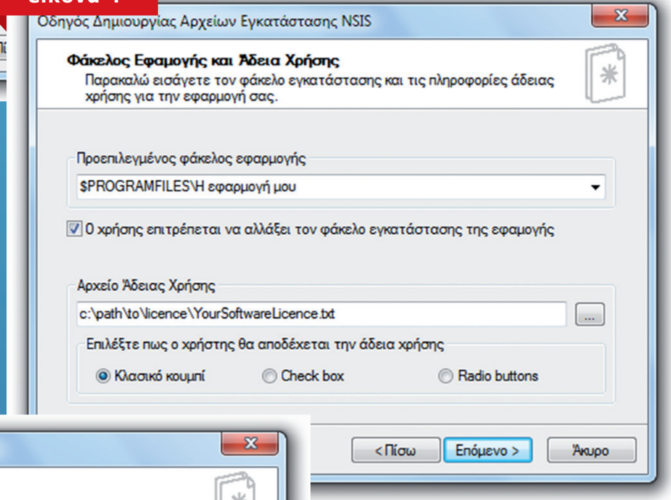
εικόνα 2



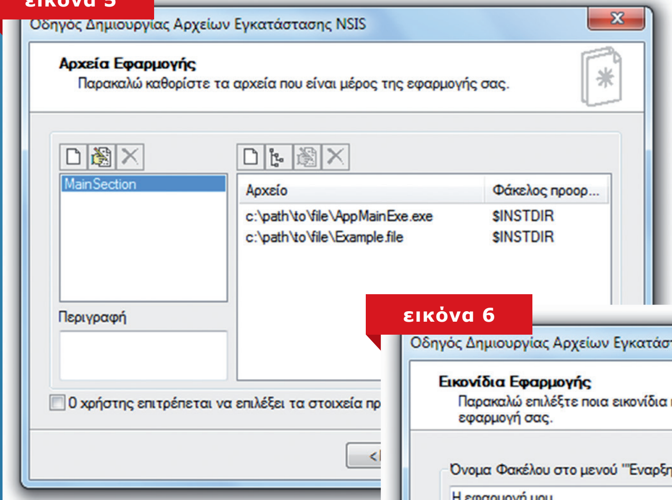
εικόνα 3



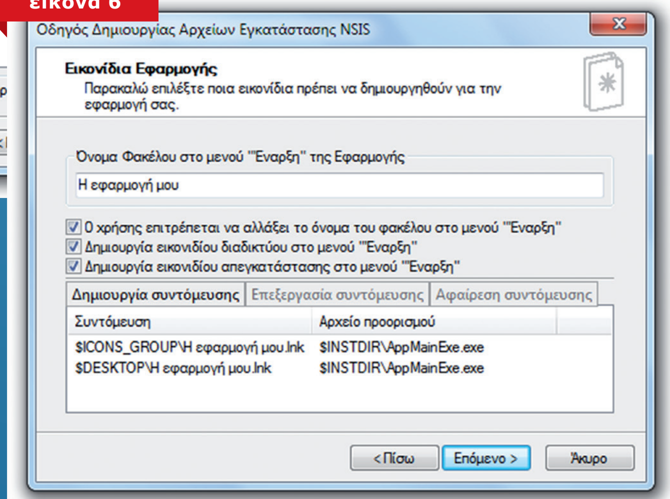
εικόνα 4



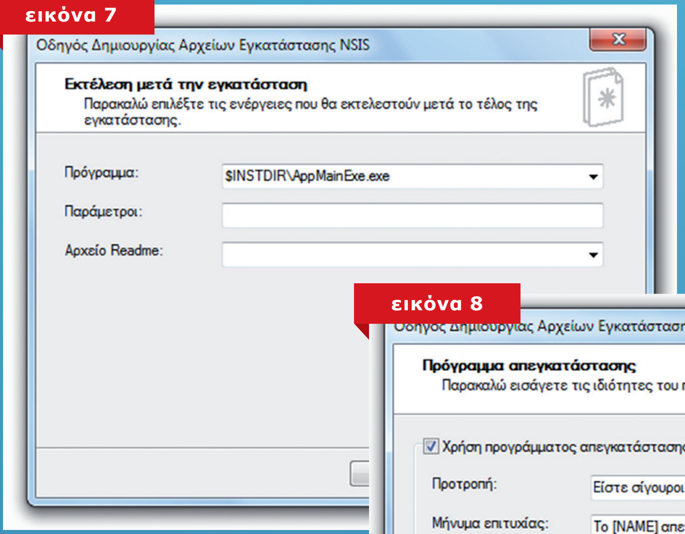
εικόνα 5



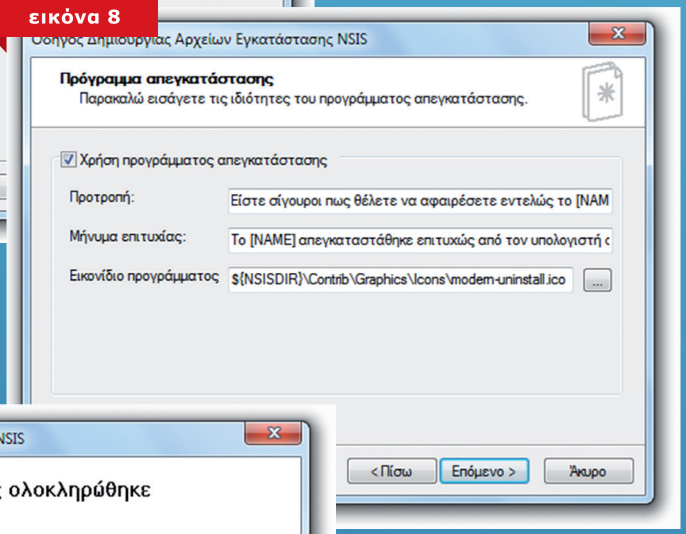
εικόνα 6



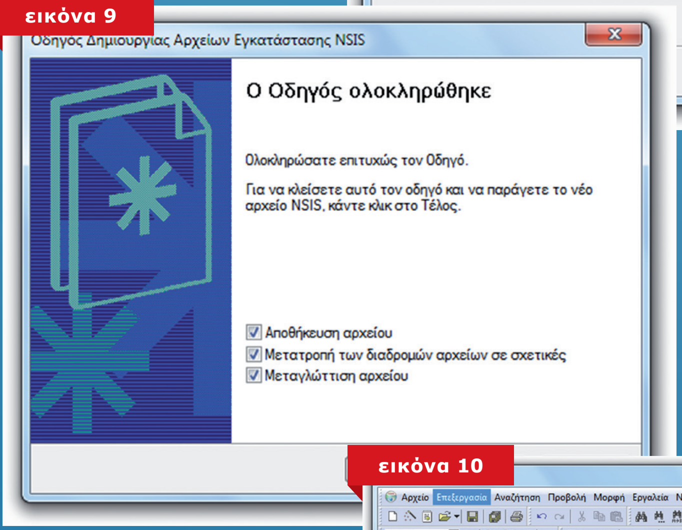
εικόνα 7



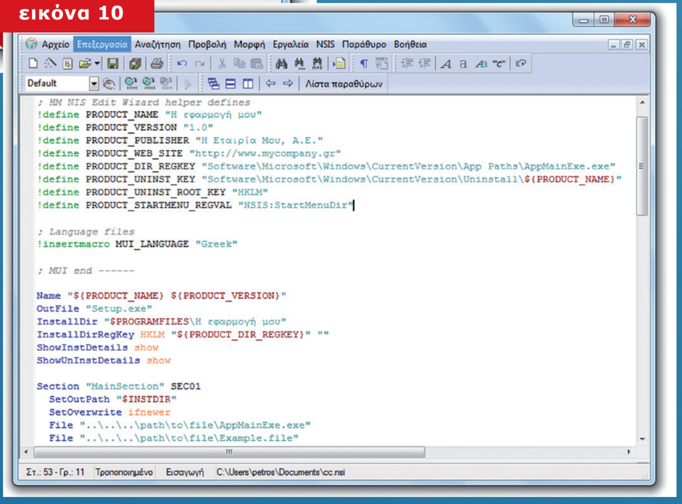
εικόνα 8



εικόνα 9



εικόνα 10



Εναλλακτικό κι εξίσου αποτελεσματικό

Ένα εναλλακτικό σύστημα για τη δημιουργία οδηγών εγκατάστασης, το οποίο μάλιστα υποστηρίζεται από μια ενθουσιώδη ομάδα, είναι το Inno Setup. Η ανάπτυξη του συγκεκριμένου συστήματος ξεκίνησε κάπου μέσα στο 1997, όταν ο αρχικός δημιουργός του (Jordan Russell) αποφάσισε να κατασκευάσει κάτι αντίστοιχο του εμπορικού InstallShield. Έκτοτε το Inno Setup εξελίσσεται συνεχώς, ενώ χάρη στον ελεύθερο διαμοιρασμό του πηγαίου του κώδικα έχουν αναπτυχθεί αρκετά παρακλάδια κι επεκτάσεις που κατά καιρούς ενσωματώνονται στον κύριο κορμό του προγράμματος. Το Inno Setup, όπως και το NSIS, λειτουργεί με τη λογική των μεταγλωττιζόμενων scripts και έχει τη δική του γλώσσα. Μάλιστα, το συντακτικό αυτής της γλώσσας είναι επηρεασμένο από την πάλαι ποτέ κραταιά Pascal (Σ.τ.Ε. Απόλυτη γλώσσα για να μάθει κάποιος προγραμματισμό, αλλά και για ν' αναπτύξει μεγάλες εφαρμογές.) Στη συνέχεια θα εξετάσουμε τη διαδικασία δημιουργίας ενός οδηγού εγκατάστασης με το Inno Setup — και τη συνδρομή ενός βοηθητικού εργαλείου.

Μπορούμε να κατεβάσουμε το Inno Setup από τη διεύθυνση `www.jrsoftware.org/isdl.php`. Η εργασία μας θα μπορούσε να ξεκινήσει αμέσως μετά την εγκατάσταση, με τη βοήθεια του Inno Setup Compiler. Πρόκειται για ένα απλοϊκό front-end για τον compiler του Inno setup, αντίστοιχο του MakeNSISW (εικόνα 11). Εμείς όμως δεν σκοπεύουμε να γράψουμε τα πάντα από την αρχή. Έτσι, όπως συνέβη και στην περίπτωση του NSIS, θα καταφύγουμε στην ευκολία ενός IDE. Θα χρησιμοποιήσουμε το Inno Script Studio, που μπορούμε να κατεβάσουμε από τη διεύθυνση `www.kymoto.org/products/Inno-script-studio/downloads`. Αφού εγκαταστήσουμε κι αυτό το εργαλείο, το ανοίγουμε κι επιλέγουμε τη δημιουργία ενός νέου project, με τη βοήθεια του σχετικού Wizard[5].

Ένας ακόμα μάγος

Μετά το τυπικό καλωσόρισμα του πρώτου βήματος, καλούμαστε να εισάγουμε τα στοιχειώδη: Το όνομα του προγράμματός μας, την έκδοσή του, το όνομα του δημιουργού και τη σχετική ιστοσελίδα (εικόνα 12). Συνεχίζοντας πρέπει να δηλώσουμε το φάκελο στον οποίο θα εγκαθίσταται εξ ορισμού το πρόγραμμά μας και ν' αποφασίσουμε αν ο χρήστης θα έχει το δικαίωμα να τον αλλάξει ή όχι (εικόνα 13). Στο επόμενο βήμα προσδιορίζουμε τα αρχεία που θα περιλαμβάνει το πακέτο, καθώς και το "κεντρικό" εκτελέσιμο αρχείο του προγράμματος που θα εγκαθίσταται. Κατά τα γνωστά, μπορούμε να επιλέξουμε και την αυτόματη εκτέλεση του προγράμματος αμέσως μετά την εγκατάσταση (εικόνα 14).

Στη συνέχεια προσδιορίζουμε τις συντομεύσεις που θέλουμε να δημιουργούνται μετά την εγκατάσταση, τόσο στο μενού Έναρξη όσο και στην Επιφάνεια Εργασίας. Εκτός από τις συντομεύσεις για το βασικό εκτελέσιμο, μπορούμε να δημιουργήσουμε κάποιες και για το εργαλείο απεγκατάστασης (εικόνα 15). Ακολουθεί το κείμενο της άδειας χρήσης και διάφορα μηνύματα που θα θέλαμε να εμφανίζονται πριν και μετά την εγκατάσταση (εικόνα 16). Λίγο πριν το τέλος συναντάμε μια λίστα με τις διαθέσιμες γλώσσες για τον οδηγό εγκατάστασης (εικόνα 17), ενώ στο τέλος καθορίζουμε τη θέση όπου θα τοποθετηθεί ο οδηγός, το αν θα χρησιμοποιεί κάποιο custom εικονίδιο κ.λπ. (εικόνα 18).

Μόλις ολοκληρώσουμε τα βήματα του οδηγού επιστρέφουμε στο βασικό παράθυρο του Inno Script Studio. Για να μεταγλωττίσουμε το script που μόλις ετοιμάσαμε, πρέ-

5. Μιλήσαμε για ευκολία και το εννοούσαμε ;)

πει να πάμε στο μενού Project και να επιλέξουμε το Compile. Αν κάνουμε κάτι τέτοιο, η διαδικασία μεταγλώττισης θα ξεκινήσει αμέσως και στο τέλος θα προκύψει ένας ωραιότατος οδηγός εγκατάστασης. Όμως το Inno Script Studio προσφέρει πολλές ακόμα δυνατότητες και θα ήταν κρίμα αν τις προσπερνούσαμε.

Βελτιώσεις και προσθήκες

Στην αριστερή περιοχή του παραθύρου του προγράμματος εμφανίζεται μια δενδροειδής δομή επιλογών. Καθεμία απ' αυτές αντιστοιχεί και σε τμήμα του script που δημιουργήσαμε προηγουμένως. Κάνοντας κλικ επάνω σε κάποια, το πρόγραμμα εμφανίζει μια σειρά επιλογών και ρυθμίσεων που αφορούν στη λειτουργία του αντίστοιχου τμήματος του script. Παρεμπιπτόντως, με κλικ στην πρώτη επιλογή της λίστας μπορούμε να δούμε ολόκληρο τον κώδικα του script (εικόνα 19). Τώρα, αν για παράδειγμα μεταβούμε στην επιλογή με τίτλο Files (εικόνα 20), θα εμφανιστεί μια λίστα με τα αρχεία που είχαμε επιλέξει νωρίτερα για ενσωμάτωση, καθώς κι ένα πλήθος επιλογών για προσθήκη νέων, αφαίρεση των υπαρχόντων, αλλαγής του ονόματος προορισμού κ.λπ. Μάλιστα, αν κάνουμε διπλό κλικ σε κάποιο από τα αρχεία της λίστας, θα δούμε ακόμα περισσότερες και πιο εξειδικευμένες επιλογές (εικόνα 21).

Ιδιαίτερο ενδιαφέρον συγκεντρώνει και η επιλογή Registry. Εκεί παρέχονται ρυθμίσεις κι επιλογές για τα κλειδιά που θα δημιουργεί ο οδηγός εγκατάστασης στο μητρώο των Windows. Αυτή η δυνατότητα είναι ιδιαίτερα χρήσιμη για ορισμένες λειτουργίες που ενδέχεται να έχει το πρόγραμμά μας ή ακόμα και για ορισμένες δικλείδες ασφαλείας. Πάντως, το πιο δυνατό σημείο του Inno Script Studio εντοπίζεται στη δυνατότητα προσθήκης των δικών μας τμημάτων κώδικα, μέσα σε script που έχουμε δημιουργήσει με τον μάγο. Για το σκοπό αυτό αρκεί να κάνουμε κλικ στην επιλογή Pascal Code και στη συνέχεια να εισάγουμε τον κώδικά μας. Σε αυτό το σημείο θα μας επιτρέψετε να εμβαθύνουμε λίγο και να δώσουμε ένα συγκεκριμένο παράδειγμα κώδικα.

Όπως ενδέχεται να παρατηρήσατε στις εικόνες των προηγούμενων βημάτων, ο οδηγός εγκατάστασης που ετοιμάσαμε προορίζεται για το πρόγραμμα AutoProcRestarter[6]. Πρόκειται για ένα πρόγραμμα που έχουμε αναπτύξει σε C# και για τη λειτουργία του απαιτεί την παρουσία του .NET framework 3.5. Σκεφτήκαμε, λοιπόν, ότι θα ήταν πολύ βολικό αν ο οδηγός εγκατάστασης ήλεγχε για την παρουσία του framework. Μάλιστα, στην περίπτωση που δεν εντόπιζε τη συγκεκριμένη έκδοση του .NET, θα μπορούσε να μας παραπέμψει στη σχετική σελίδα της Microsoft για τη λήψη του. Για να προσθέσουμε αυτή τη λειτουργικότητα στον οδηγό εγκατάστασης γράψαμε ένα μικρό τμήμα κώδικα σε Pascal, το οποίο ενσωματώσαμε στο έτοιμο script. Γι' αυτή την ενσωμάτωση επιλέξαμε το Pascal Code. Δείτε τον κώδικα που γράψαμε:

```
function InitializeSetup(): Boolean;
var
  ErrorCode: Integer;
  netFrameWorkInstalled : Boolean;
  isInstalled: Cardinal;
begin
```

6. Μια μικρή εφαρμογή που έχει αναπτύξει ο γράφων, η οποία κατοικεί στο system tray και μπορεί σε τακτά χρονικά διαστήματα να επανεκκινεί την εφαρμογή που του έχουμε υποδείξει. Περισσότερα μπορείτε να βρείτε στη σελίδα http://www.multipetros.gr/?p=1854.

```
  result := true;

  // Check for the .Net 3.5 framework
  isInstalled := 0;
  netFrameworkInstalled := RegQueryDWordValue(HKLM,'SOFTWARE\Microsoft\
  NET Framework Setup\NDP\v3.5','Install', isInstalled);
  if ((netFrameworkInstalled)  and (isInstalled <> 1))
  then netFrameworkInstalled := false;

  if netFrameworkInstalled = false then
  begin
  if (MsgBox(ExpandConstant('{cm:dotnetmissing}'),
  mbConfirmation, MB_YESNO) = idYes) then
    begin
      ShellExec('open', 'http://www.microsoft.com/
      downloads/details.aspx?FamilyID=333325fd-ae52-
      4e35-b531-508d977d32a6&DisplayLang=en', '','',SW_
      SHOWNORMAL,ewNoWait,ErrorCode);
    end;
    result := false;
  end;

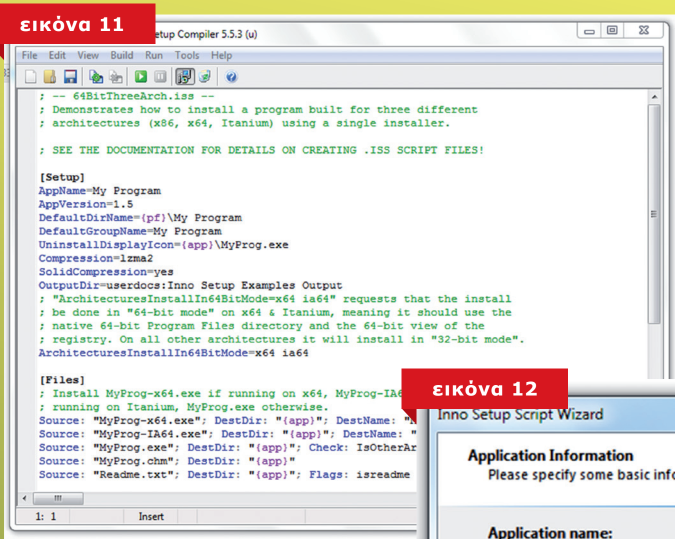
end;
```

Η πλήρης κατανόηση του κώδικα προϋποθέτει τη γνώση της Pascal. Ωστόσο, πιστεύουμε ότι όλοι μπορούν να κατανοήσουν τη λειτουργία του σε γενικές γραμμές. Φυσικά, το παραπάνω τμήμα κώδικα συνιστά ένα πολύ μικρό δείγμα των δυνατοτήτων που ξετυλίγονται μπροστά μας. Περισσότερες λεπτομέρειες γύρω από τη γλώσσα του Inno Setup θα βρείτε στη διεύθυνση www.jrsoftware.org/ishelp/index.php?topic=scriptcreating.

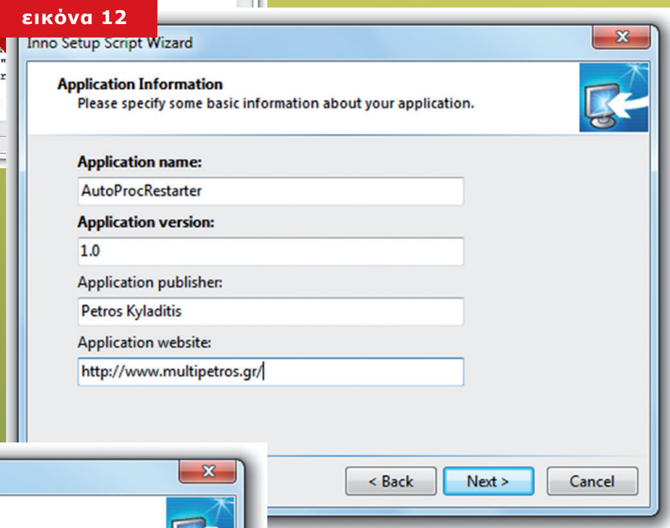
Εισαγωγή!

Όχι, δεν πρόκειται περί λάθους. Το ταξίδι στο συναρπαστικό κόσμο των οδηγών εγκατάστασης ξεκινάει τώρα. Αν αναλογιστούμε ότι ο οδηγός εγκατάστασης είναι το τελευταίο πράγμα που πρέπει να φτιάξει ο developer (ενδεχομένως υπό πίεση και κουβαλώντας αρκετή κούραση), ενώ την ίδια στιγμή αποτελεί το πρώτο που θα δει ο χρήστης, καταλαβαίνουμε εύκολα ότι αξίζει να αφιερώσουμε αρκετό χρόνο στο ζήτημα. Κάτι ακόμα που μπορούμε να καταλάβουμε, είναι ότι τα προγράμματα που παρουσιάσαμε αποτελούν ευλογία :D Επενδύστε λίγο χρόνο για την εξοικείωση μαζί τους και είμαστε σίγουροι ότι θα μας θυμηθείτε.

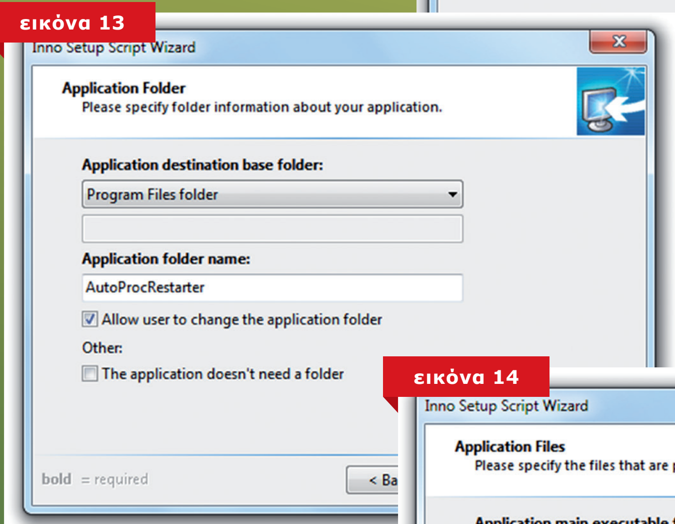
εικόνα 11



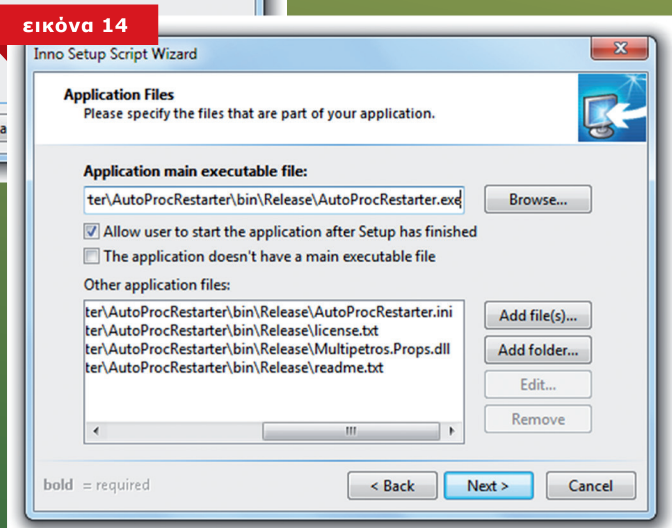
εικόνα 12



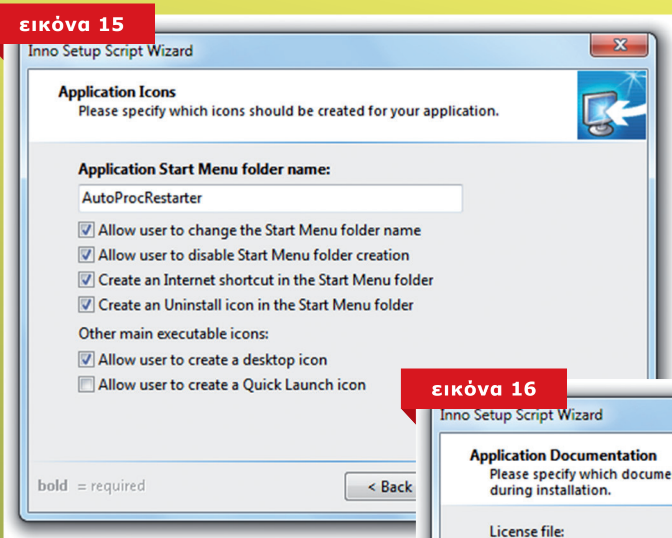
εικόνα 13



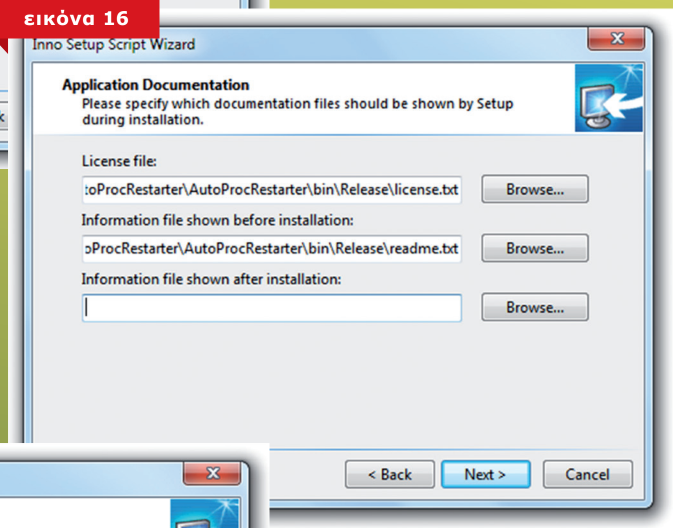
εικόνα 14



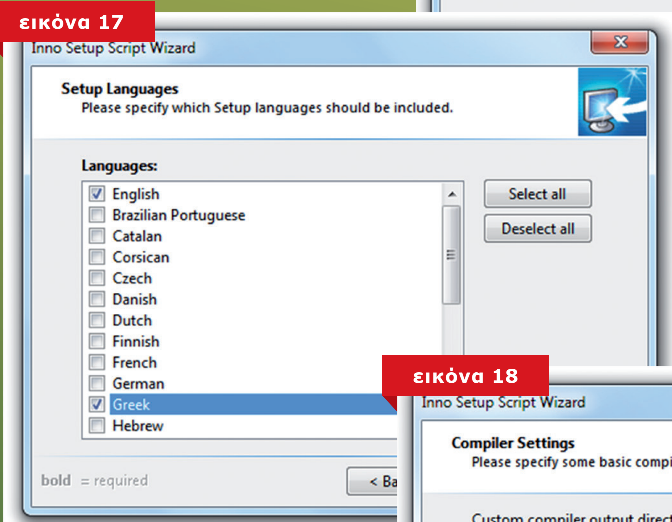
εικόνα 15



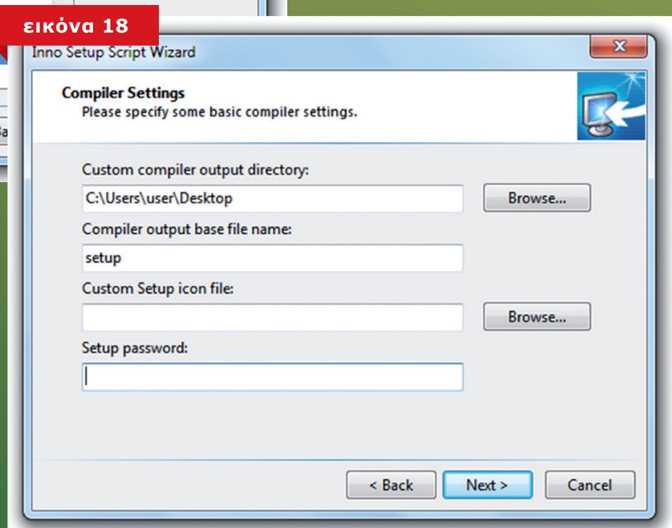
εικόνα 16



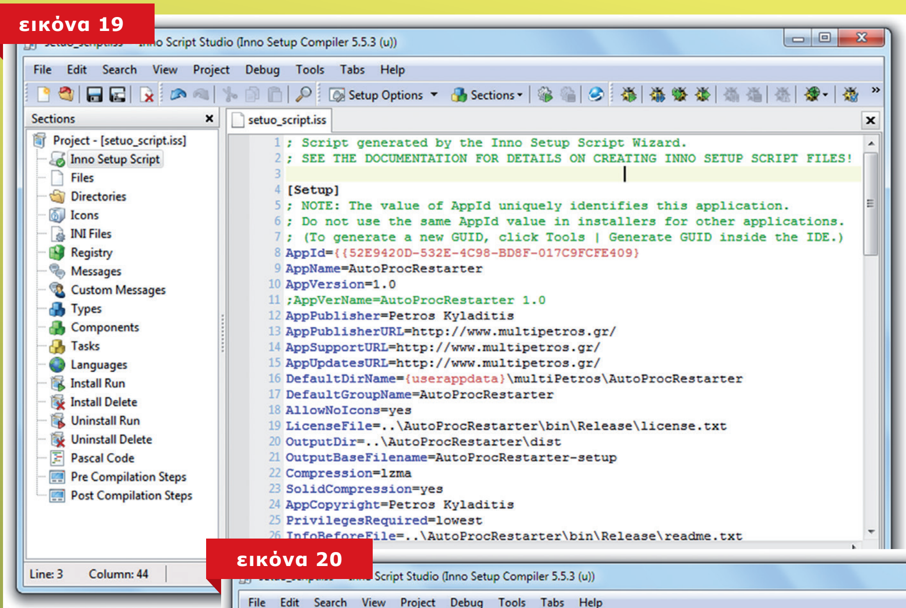
εικόνα 17



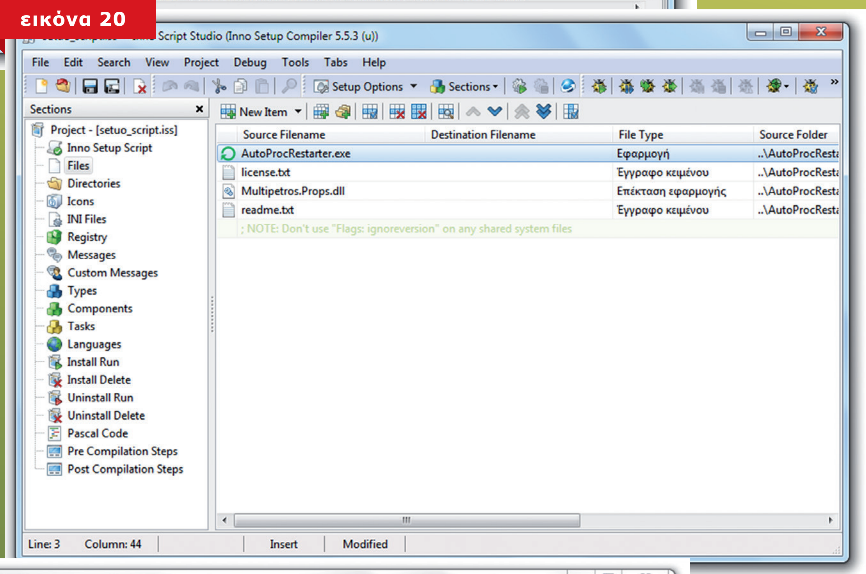
εικόνα 18



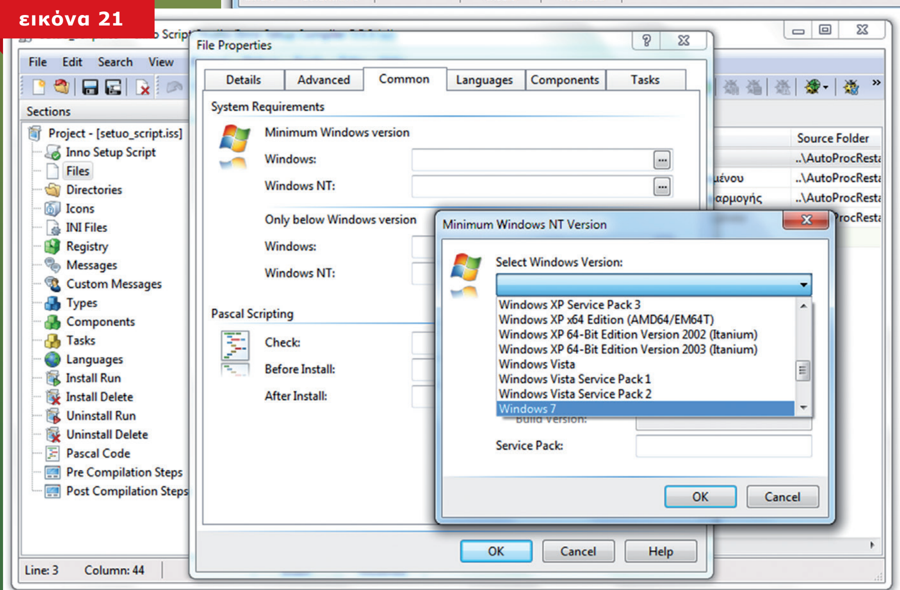
εικόνα 19



εικόνα 20



εικόνα 21



Skill: Intermediate
Tags: IDS, IPS, Snort, Oinkcode, VRT rules, Emerging Threats, pfSense

by subZraw



Εντοπισμός εισβολέων, στο επίπεδο του router!

Ποιο είναι το μεγάλο "συν" κάθε οικιακού router, ασχέτως του κόστους, των επιμέρους δυνατοτήτων ή της φήμης του κατασκευαστή; Μα το γεγονός ότι λειτουργεί ως firewall, για τις συσκευές και τους υπολογιστές πίσω του. Όσοι βέβαια βλέπουν το όλο θέμα της ασφάλειας *λίγο* πιο σοβαρά από το Μέσο Παπαδόπουλο (TM), τότε κατά πάσα πιθανότητα θα σνομπάρουν τόσο το firewall, όσο και τον ίδιο τον οικιακό router.

Όχι ότι δεν υπάρχουν αξιόλογοι home routers στην αγορά, αλλά όποιος έχει υλοποιήσει μια λύση βασισμένη σε εξειδικευμένο λειτουργικό σύστημα, όπως, π.χ., είναι το λατρευτό pfSense, δύσκολα γυρίζει πίσω. Για το pfSense έχουμε πει και γράψει πολλά στο παρελθόν και σίγουρα θα πούμε και θα γράψουμε κι άλλα στο μέλλον (βλ., π.χ., το http://deltahacker.gr/deltacast-s01e07 ή το http://deltahacker.gr/openvpn-pfsense). Σ' αυτό το άρθρο θέλουμε να εστιάσουμε στο πώς ενισχύουμε ακόμα περισσότερο την ασφάλεια του δικτύου πίσω από ένα pfSense box, επιστρατεύοντας ένα ικανό σύστημα intrusion detection και prevention. Πιο συγκεκριμένα, σε λίγο θα γνωρίσουμε το Snort κι αμέσως μετά θα το εγκαταστήσουμε και ρυθμίσουμε, καθώς και παρακολουθήσουμε επί τω έργω. Πρώτα απ' όλα όμως οφείλουμε να εξηγήσουμε τι είναι ένα σύστημα intrusion detection ή/και prevention.

IDS, IPS, IDPS, firewalls και τα ρέστα

Ένα Intrusion Detection System, εν συντομία IDS, είναι μια συσκευή ή εφαρμογή λογισμικού με αποστολή τον εντοπισμό κακόβουλων ενεργειών ή/και παραβιάσεων πολιτικών που αφορούν σ' ένα μεμονωμένο σύστημα ή σ' ένα ολόκληρο δίκτυο. Κάθε φορά που το IDS ανιχνεύει κάτι παράξενο ή παράτυπο στο σύστημα ή στο δίκτυο που εποπτεύει, ετοιμάζει και μια σχετική αναφορά. Όλες αυτές οι αναφορές είναι διαθέσιμες στον υπεύθυνο ή στους υπεύθυνους διαχειριστές, οι οποίοι αφού τις αξιολογήσουν αποφασίζουν για το αν πρέπει να πάρουν μέτρα προς την ενίσχυση της ασφάλειας ή/και να φροντίσουν για την εφαρμογή προαποφασισμένων πολιτικών.

Υπάρχουν δύο είδη IDS: Εκείνα που παρακολουθούν ένα μόνο μηχάνημα (Host-based Intrusion Detection System, HIDS), καθώς κι εκείνα που εποπτεύουν ένα ολόκληρο δίκτυο (Network-based Intrusion Detection System, NIDS). Το Snort, με το οποίο θα ασχοληθούμε σε πολύ λίγο, ανήκει στη δεύτερη κατηγορία. Πρόκειται δηλαδή για ένα NIDS, αλλά έχει την ικανότητα να λειτουργεί κι ως Intrusion Prevention System (IPS). Τα δε IPS είναι κοντινοί συγγενείς των IDS, μόνο που δεν περιορίζονται στην παθητική παρατήρηση κι αναφορά: Σε αντίθεση με ένα IDS, κάθε φορά που ένα IPS ανιχνεύει μια επίθεση ή παραβίαση, ενεργοποιεί μηχανισμούς αναχαίτισης. Ακριβώς γι' αυτό, τα IPS αναφέρονται κι ως IDPS (Intrusion Detection *and* Prevention System).

Πριν στρέψουμε την προσοχή μας ειδικά στο Snort, θεωρούμε ότι πρέπει ν' απαντήσουμε σ' ένα εύλογο ερώτημα: Ποια είναι η διαφορά ενός IDPS από ένα firewall;

Λοιπόν, χαιρόμαστε που ρωτήσατε.

Ένα τυπικό firewall σε κάποιο σύστημα ή δίκτυο, έχει μια προκαθορισμένη συμπεριφορά και στην πλειονότητα των περιπτώσεων φιλτράρει κυρίως τα εισερχόμενα πακέτα. Αναλυτικότερα, αν ένα εισερχόμενο πακέτο δεν κατευθύνεται σε ανοικτό port, τότε αμέσως απορρίπτεται. Ένα IDPS λειτουργεί αρκετά πιο περίπλοκα. Κατ' αρχάς, ακόμη κι όταν βλέπει εισερχόμενα πακέτα προς ανοικτά ports, αν διαπιστώσει ότι λαμβάνει χώρα μια κακόβουλη ενέργεια, όπως, π.χ., είναι ένα DoS ή κάποιο brute force attack, αναφέρει το γεγονός ή/και μπλοκάρει τα εμπλεκόμενα remote hosts. Επιπρόσθετα, ένα IDPS είναι δυνατόν να ελέγχει και τα πακέτα που διακινούνται εντός δικτύου, καθώς και τα εξερχόμενα, δηλαδή αυτά που ξεκινούν από μηχανήματα του τοπικού δικτύου και φεύγουν προς τον έξω κόσμο. Γιατί είναι χρήσιμο αυτό; Μα, γιατί σε αντίθεση με το οικιακό μας δίκτυο, στο δίκτυο μιας εταιρείας, ενός οργανισμού ή κάποιου εργαστηρίου, οι χρήστες δεν επιτρέπεται να κάνουν ό,τι θέλουν. Και σ' αυτά τα "ό,τι θέλουν" δεν συγκαταλέγονται μόνο κατάφωρα κακόβουλες ενέρ-

γειες, όπως, π.χ., είναι μια επίθεση brute force, αλλά κι απλές, ενδεχομένως αθώες ενέργειες, οι οποίες όμως αποτελούν παραβιάσεις προαποφασισμένων πολιτικών. (Παράδειγμα: Απογορεύεται η χρήση του Dropbox ή εφαρμογών που χρησιμοποιούν το πρωτόκολλο BitTorrent, όπως είναι το Sync.)

Γενικά, μπορούμε να φανταζόμαστε ότι τα IDPS αποτελούν ένα είδος application-level firewall. Εξετάστε ένα οποιοδήποτε από τα πολλά firewalls τρίτων κατασκευαστών που διατίθενται για Windows κι αναλογιστείτε τι κάνει: Θα διαπιστώσετε ότι η λειτουργικότητά του θυμίζει εκείνη ενός IDPS. Κάποιοι κατασκευαστές μάλιστα το αναφέρουν ξεκάθαρα: "Έχουμε *και* IPS / υπερέχουμε των άλλων / προτιμήστε μας" (ή κάπως έτσι, τέλος πάντων). Η κρίσιμη διαφορά εδώ είναι ότι τα application-level firewalls για Windows προστατεύουν ένα μόνο μηχάνημα, τη στιγμή που ένα τυπικό IDPS κατά πάσα πιθανότητα θα προστατεύει ένα ολόκληρο δίκτυο.

Υπάρχουν πάρα πολλά ακόμα που θα μπορούσαμε να συζητήσουμε για τα IDS/IPS, όπως, π.χ., για τις μεθόδους ελέγχου που χρησιμοποιούν ή για το πόσο ακριβή (δεν) είναι. Όλα αυτά όμως είναι καλύτερα να τα δούμε στην πράξη, παίζοντας με το πανίσχυρο Snort μέσα από το web panel του pfSense.

Πρώτη γνωριμία με το Snort

Πρόκειται για ένα εξαιρετικά δημοφιλές IDS και IPS (IDPS), που λειτουργεί σε επίπεδο δικτύου (`https://www.snort.org`). Αποτελεί Ανοικτό Λογισμικό, διατίθεται δωρεάν και ξεκίνησε ν' αναπτύσσεται το 1998 από τον Martin Roesch. Αργότερα συνέχισε στους κόλπους της εταιρείας Sourcefire, την οποία ίδρυσε ο ίδιος ο Roesch. Τον Οκτώβριο του 2013 η Sourcefire αγοράστηκε από τη Cisco Systems και πλέον ο Roesch διατελεί αντιπρόεδρος και chief architect του Security Business Group της εταιρείας.

Το Snort λειτουργεί σε δίκτυα που βασίζονται στο πρωτόκολλο IP και είναι ικανό για ανάλυση και καταγραφή των διακινούμενων πακέτων σε πραγματικό χρόνο. Μεταξύ άλλων, η εφαρμογή διακρίνει απόπειρες ή προπομπούς επιθέσεων (π.χ., port scans), καθώς και επιθέσεις σε εξέλιξη (π.χ., DoS attacks). Μπορεί δε να συμπεριφέρεται ως sniffer, ως packet logger ή ως ένα πλήρες IDS — προαιρετικά και με ικανότητες intrusion prevention.

Όταν το Snort λειτουργεί ως sniffer, τότε απλά διαβάζει όλα τα διακινούμενα δικτυακά πακέτα και τα εμφανίζει στην κονσόλα. Επιπρόσθετα, όταν του ζητείται να τρέχει ως packet logger, τότε τα πακέτα που διαβάζει τα αποθηκεύει σε αρχεία καταγραφής, στο δίσκο του συστήματος. Τέλος, όταν το Snort έχει χρέη IDS, τότε παρακολουθεί όλη τη δικτυακή κίνηση και την αναλύει με βάση ένα σύνολο κανόνων που έχει ορίσει ή υποδείξει ο χρήστης. Αναλόγως των επιταγών του τελευταίου, το Snort αναλαμβάνει και συγκεκριμένες δράσεις, όπως, π.χ., μπλοκάρισμα συγκεκριμένων hosts για προκαθορισμένο χρόνο.

Το Snort τρέχει από την κονσόλα απλού κειμένου και δεν παρέχει κάποιο web panel ή front-end γραφικών. Βεβαίως, ο υπολογιστής ο οποίος το φιλοξενεί οφείλει να βρίσκεται σε κάποια τοπολογικά προνομιακή θέση, υπό την έννοια ότι όλη η δικτυακή κίνηση πρέπει να διέρχεται απ' αυτόν. Τυπικά, στην περίπτωση ενός απλού δικτύου το Snort λειτουργεί στο επίπεδο του router. Για το pfSense μάλιστα διατίθεται έτοιμο πακέτο (PBI) με το Snort, οπότε σε πολύ λίγο θα γνωρίσουμε την εφαρμογή μέσα από το γνώριμο και λειτουργικό web panel του pfSense. Αν μη τι άλλο, λοιπόν, η πρώτη μας γνωριμία με το Snort θα είναι ομαλή, αφού δεν θα χρειαστεί να κατα-

φύγουμε στην κονσόλα. Σημειώστε επίσης πως οποιαδήποτε στιγμή θελήσουμε να εμβαθύνουμε, τότε γρήγορα θα διαπιστώσουμε ότι το παρεχόμενο από to pfSense web panel, μόνο περιοριστικό δεν είναι.

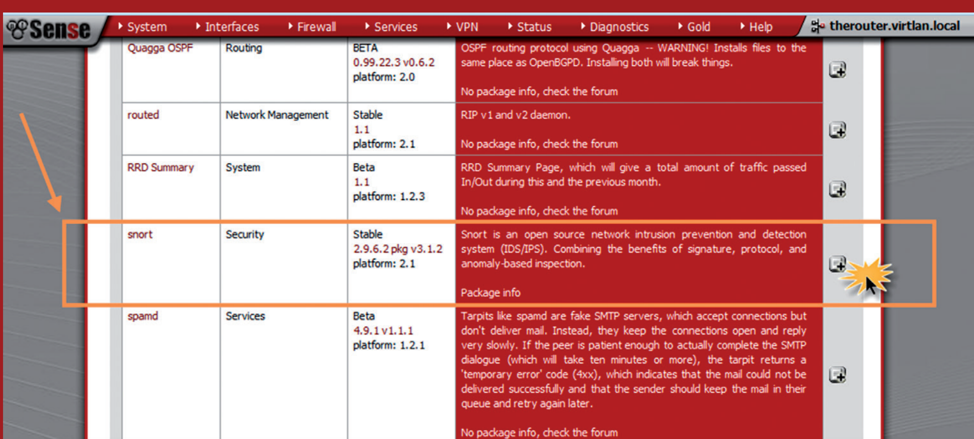
Εγκατάσταση Snort στο pfSense

Αφού συνδεθούμε στο web panel του pfSense από τον browser της προτίμησής μας, πρώτη μας φροντίδα είναι η εγκατάσταση του Snort. Δείτε τα screenshots και διαβάστε τις αντίστοιχες περιγραφές.

Σημείωση 1. *Για την ομαλή λειτουργία του Snort, το pfSense box καλό είναι να 'χει 2GB μνήμης RAM ή περισσότερα και γύρω στα 8GB ελεύθερα στο δίσκο του. Βεβαίως, περισσότερη RAM ή/και ελεύθερος χώρος στο δίσκο δε βλάπτουν.*

Σημείωση 2. *Τα ακόλουθα screenshots είναι από VM που στήσαμε για τις ανάγκες της παρουσίασης. Προς το τέλος του άρθρου παρατίθενται και screenshots από το Snort που λειτουργεί στο φυσικό pfSense box, το οποίο χρησιμοποιούμε για την προστασία του τοπικού μας δικτύου.*

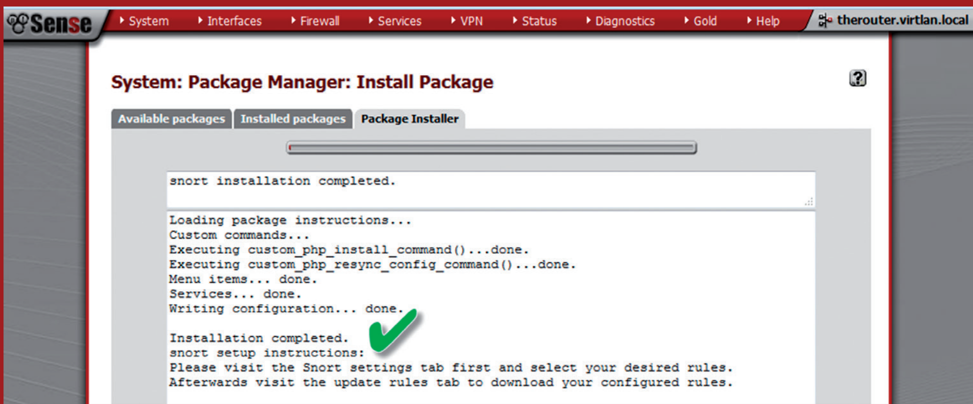
Ξεκινάμε ακολουθώντας τη διαδρομή System → Packages → Available Packages. Στη λίστα με τα διαθέσιμα πακέτα υπάρχει κι εκείνο του Snort. Ζητάμε την εγκατάστασή του μ' ένα κλικ στο κουμπάκι [+], στα δεξιά της γραμμής του.



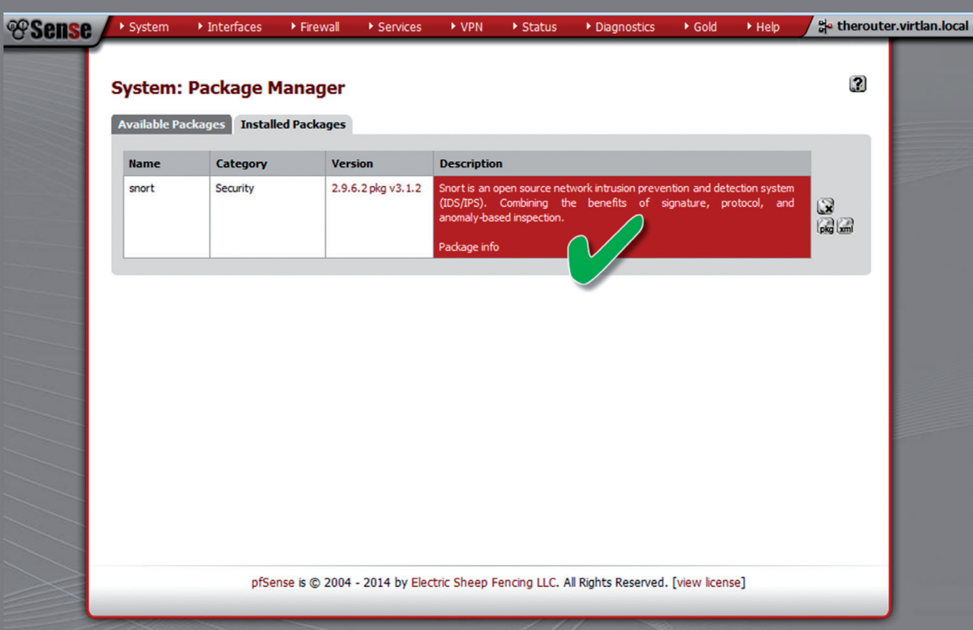
Πριν ξεκινήσει η εγκατάσταση, το pfSense χρειάζεται επιβεβαίωση από μέρους μας. Του τη δίνουμε με κλικ στο κουμπί [Confirm].



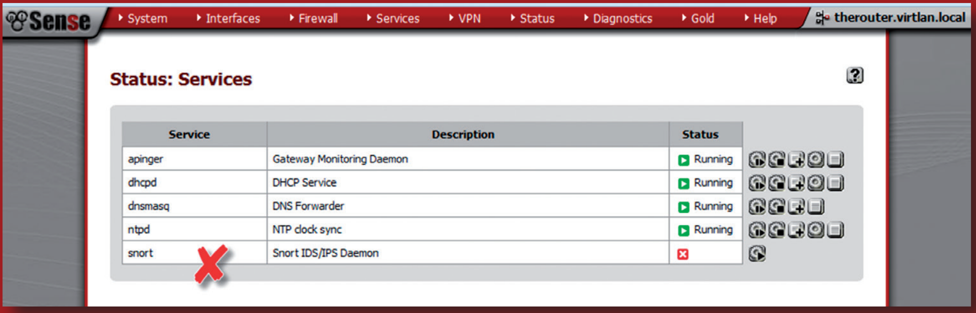
Η εγκατάσταση ίσως χρειαστεί λίγη ώρα για να ολοκληρωθεί. Όσο διαρκεί δεν χρειάζεται να κάνουμε κάτι, μιας και η σχετική διαδικασία είναι εντελώς αυτοματοποιημένη. Μετά το πέρας της θα δούμε το μήνυμα "Installation completed".



Αν όλα έχουν πάει καλά —και δεν βλέπουμε το λόγο για το αντίθετο— στην καρτέλα Installed Packages του Package Manager θα πρέπει να φιγουράρει (και) το Snort.



Αν από το μενού του pfSense δώσουμε Status → Services, θα δούμε ότι το Snort ναι μεν συγκαταλέγεται στις υπηρεσίες που προσφέρει ο router μας, δεν είναι όμως ενεργό. Λογικό, αφού πρώτα οφείλουμε να το ρυθμίσουμε.



Βασική ρύθμιση κι ενημέρωση

Το Snort είναι σε θέση να παρακολουθεί ένα ή περισσότερα network interfaces του μηχανήματος στο οποίο τρέχει. Κάθε pfSense box διαθέτει τουλάχιστον δύο interfaces: το WAN και το LAN. Για τις ανάγκες ενός μικρού δικτύου συνήθως δεν μας ενδιαφέρει τι κάνουν οι συσκευές πίσω από τον router, μ' άλλα λόγια αυτές που έχουν μπροστά τους το LAN interface. Δεν έχει λοιπόν νόημα να πούμε στο Snort να παρακολουθεί το LAN. Μας ενδιαφέρει όμως πολύ το τι γίνεται με την κίνηση που έρχεται από τον έξω κόσμο προς τα μέσα, επομένως οπωσδήποτε θέλουμε το Snort να παρακολουθεί το WAN interface. Για τη ρύθμιση του Snort, από το μενού του pfSense δίνουμε Services → Snort. Δείτε τα ακόλουθα screenshots και φυσικά διαβάστε τις αντίστοιχες περιγραφές.

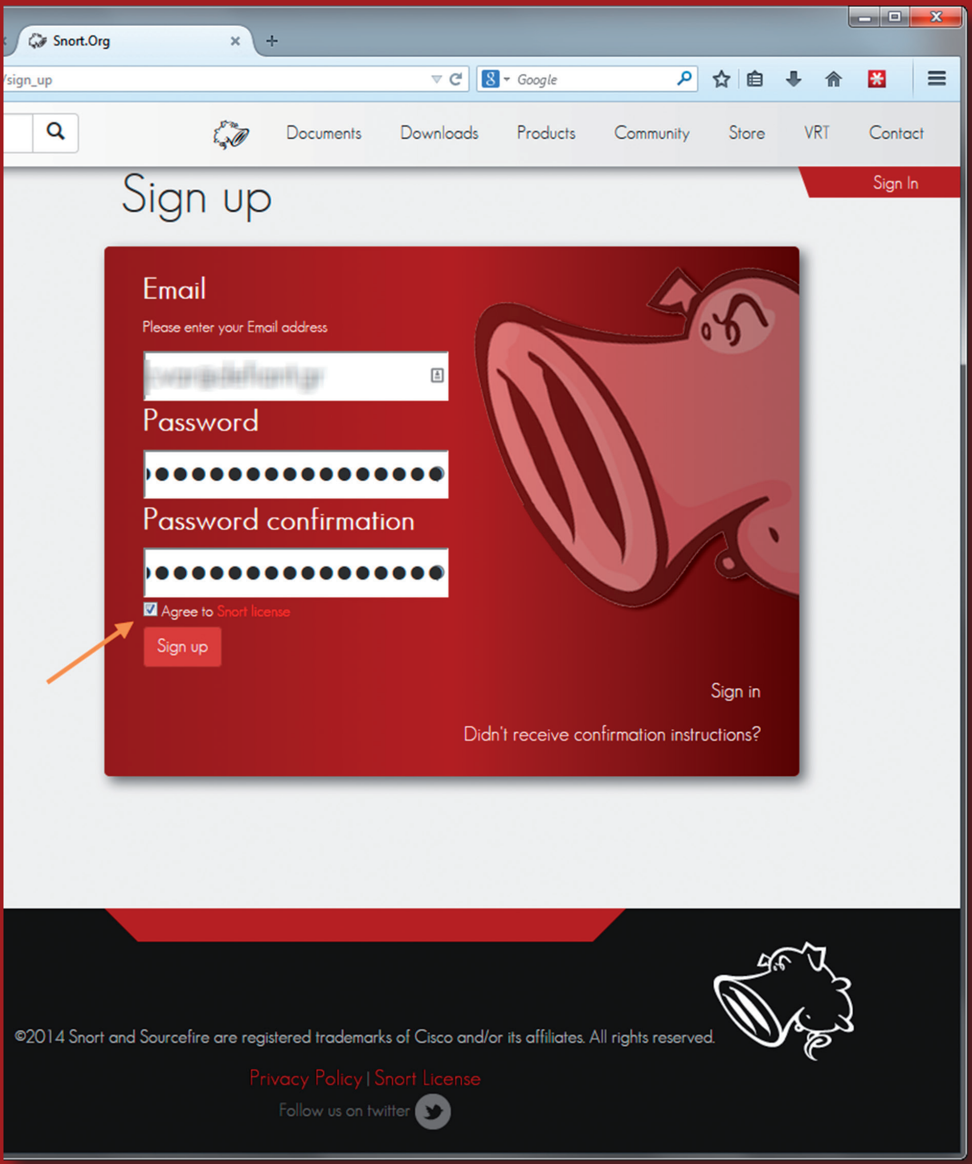
Πριν ορίσουμε το interface ή τα interfaces που θα παρακολουθεί το Snort, υπάρχουν κάποιες γενικές ρυθμίσεις που οφείλουμε να διευθετήσουμε. Κάνουμε κλικ στην καρτέλα Global Settings.



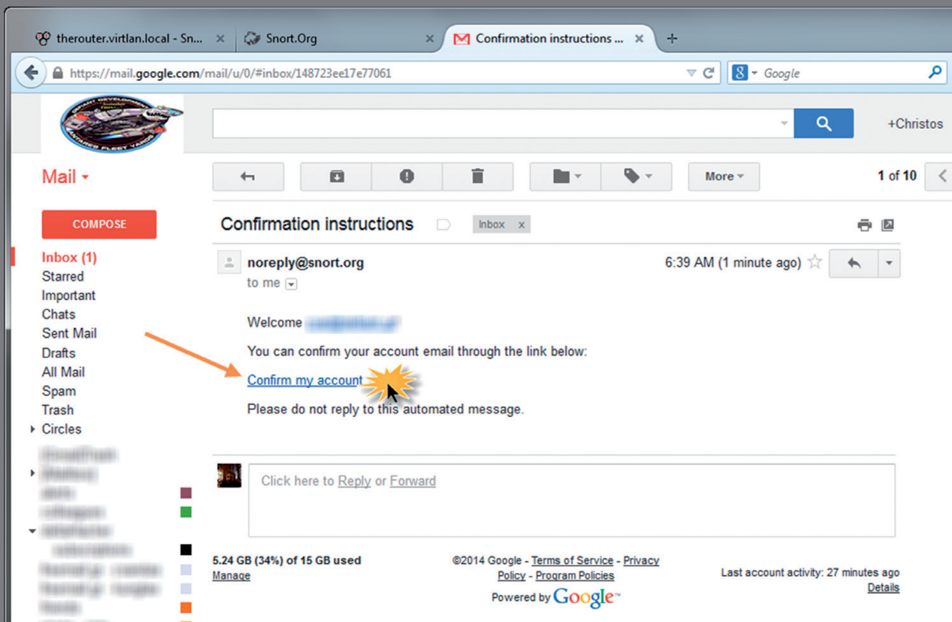
Εδώ φαίνεται ότι έχουμε αρκετή δουλειά, ετυχώς όμως τα πράγματα είναι πολύ πιο απλά απ' όσο δείχνουν. Πριν όμως πειράξουμε οτιδήποτε, ας αποκτήσουμε ένα Oinkcode για τη λήψη κανόνων...



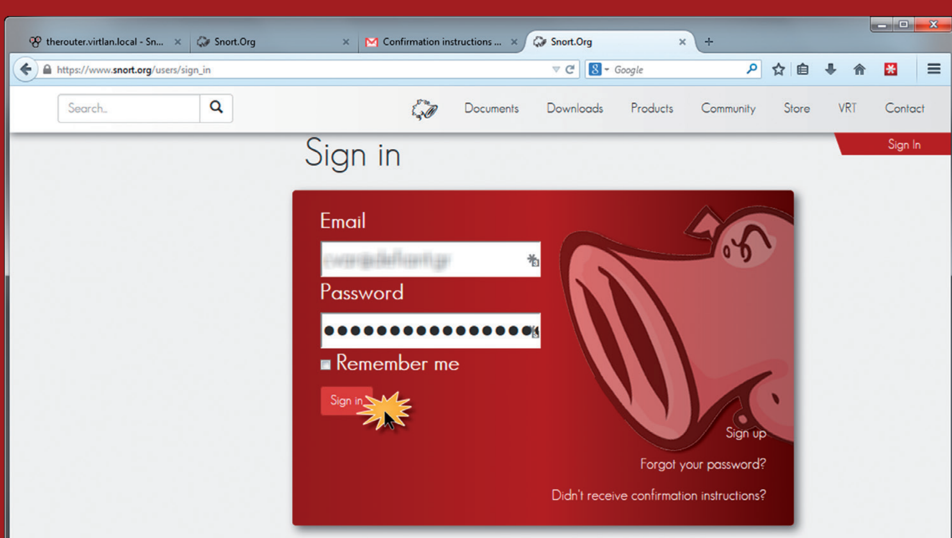
Από τη στιγμή που έχουμε το δικό μας Oinkcode, είμαστε σε θέση να κατεβάζουμε πακέτα με κανόνες για το Snort. Το Oinkcode δεν είναι τίποτε άλλο από ένα αλφαριθμητικό που αντιστοιχεί σ' ένα λογαριασμό χρήστη, ο οποίος βρίσκεται στο δικτυακό τόπο του Snort (https://www.snort.org). Οι εν λόγω λογαριασμοί είναι δωρεάν και για να δημιουργήσουμε τον δικό μας αρκεί να πάμε στο https://www.snort.org/users/sign_up (Μη ξεχάσετε να τσεκάρετε το "Agree to Snort license".)



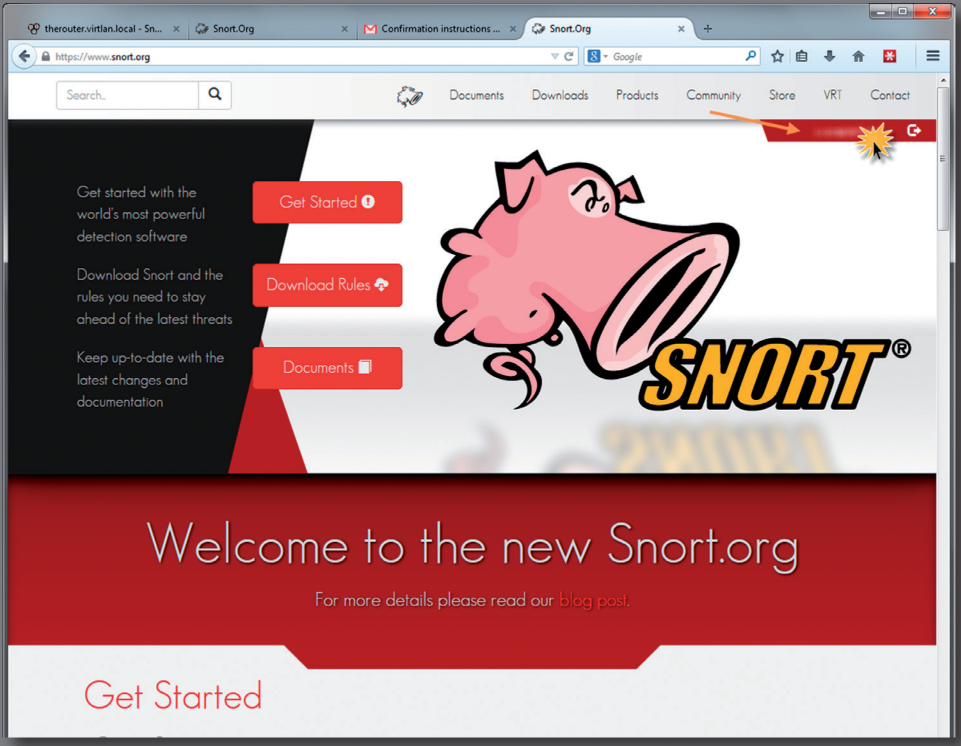
Κατά τη δημιουργία λογαριασμού δίνουμε μια *έγκυρη* διεύθυνση email. Σ' αυτή θα λάβουμε ένα μήνυμα επιβεβαίωσης.



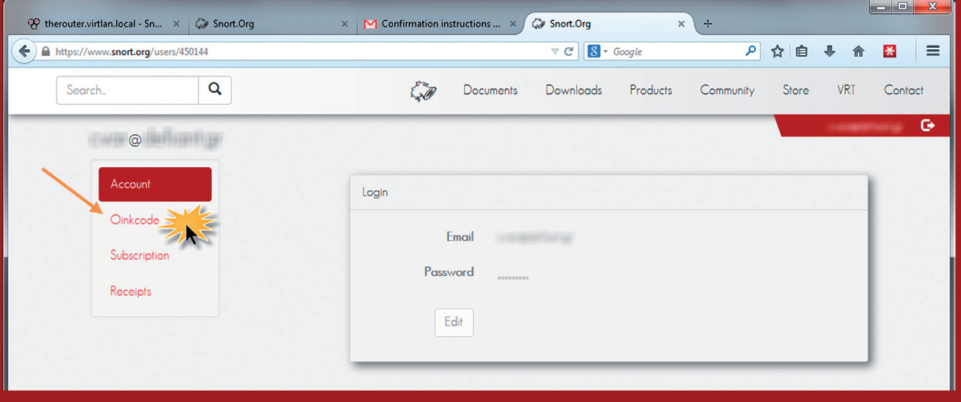
Με κλικ στο σύνδεσμο του μηνύματος επιβεβαίωσης οδηγούμαστε στη σελίδα Sign in, στο site του Snort. Αφού πληκτρολογήσουμε το email και το password, συνδεόμαστε για πρώτη φορά στο λογαριασμό μας.



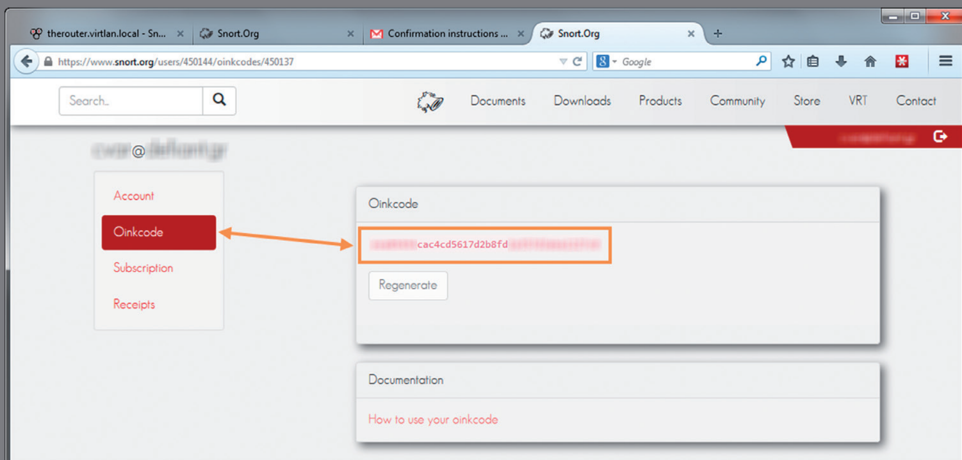
Μετά τη σύνδεση, πάνω δεξιά στη σελίδα υποδοχής υπάρχει ένα link με το email μας. Κάνουμε κλικ πάνω του...



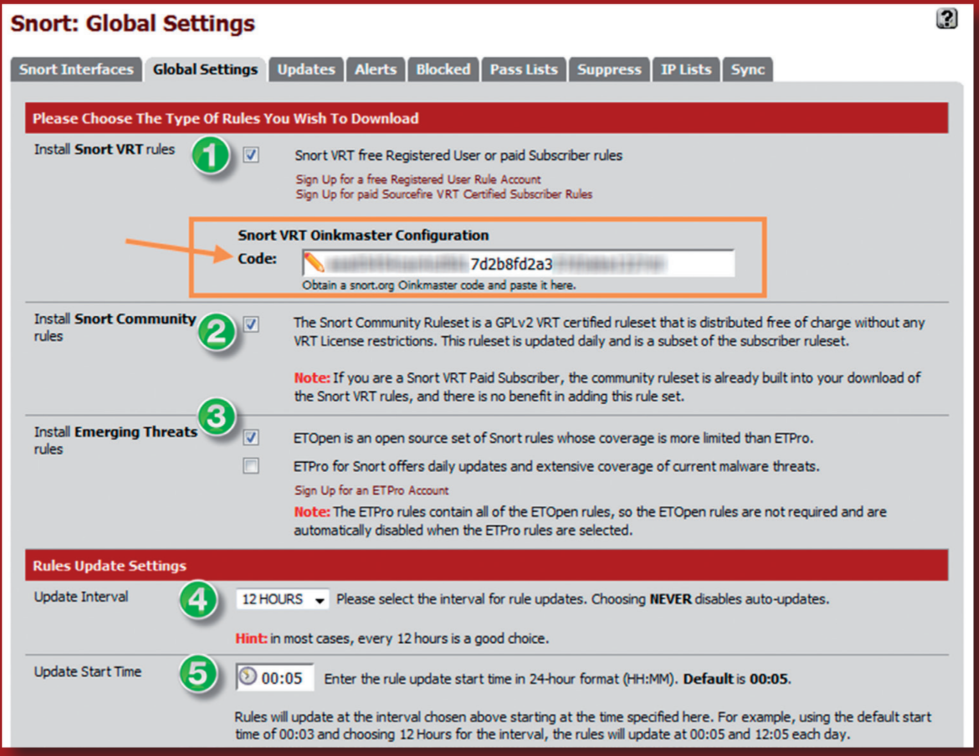
...και στη νέα σελίδα που εμφανίζεται άλλο ένα κλικ πάνω στο Oinkcode.



Ιδού το Oinkcode του λογαριασμού μας! Μπορούμε αν θέλουμε να παραγάγουμε ένα άλλο, με κλικ στο κουμπί [Regenerate]. Αλλά δεν έχουμε λόγο για να κάνουμε κάτι τέτοιο. Αντίθετα, αυτό που χρειάζεται να κάνουμε είναι να επιλέξουμε το υπάρχον Oinkcode και να το αντιγράψουμε (π.χ., με [CTRL+C] και [CTRL+V]) στο πρόχειρο ή σ' ένα text file, γιατί σε λίγο θα το δώσουμε στο Snort.



Στο web panel του pfSense, και συγκεκριμένα στην καρτέλα Global Settings του Snort, φροντίζουμε ώστε να 'ναι τσεκαρισμένη η επιλογή Install Snort VRT rules (1). Στη θυρίδα ονόματι Code, από κάτω, αντιγράφουμε το Oinkcode μας. Ως κάτοχοι έγκυρου Oinkcode μπορούμε να λαμβάνουμε ενημερωμένα —δωρεάν ή επί πληρωμή— σύνολα κανόνων, τα οποία βοηθούν την εφαρμογή ν' ανιχνεύει malware, απόπειρες επιθέσεων και γενικά να αντιλαμβάνεται συμπεριφορές που θα μπορούσαν να 'ναι επιβλαβείς για το δίκτυό μας. Σημειώστε ότι αυτό το "VRT" αποτελεί ακρωνύμιο του Vulnerability Research Team και είναι το όνομα της ομάδας διαχείρισης των λεγόμενων VRT rules της Sourcefire. Στη συνέχεια, τσεκάρουμε το κουτάκι δεξιά στο Install Snort Community rules (2). Πρόκειται για ένα δωρεάν αλλά επίσημα συντηρούμενο σύνολο κανόνων, το οποίο καλύπτεται από την άδεια χρήσης GPLv2 κι ενημερώνεται σε καθημερινή βάση. Τσεκάρουμε και το Install Emerging Threats rules (3), ώστε επιπρόσθετα να λαμβάνουμε και το δωρεάν σύνολο κανόνων ETOpen, για τον εντοπισμό malware και exploits. Παρατηρήστε ότι υπάρχει και το ETPro, το οποίο αποτελεί υπερσύνολο του ETOpen. Εκτός του ότι είναι πιο διευρυμένο, το ETPro εμπλουτίζεται σε καθημερινή βάση (βλ. http://emergingthreats.net/products/etpro-ruleset). Για το ETPro απαιτείται επί πληρωμή συνδρομή, η οποία ξεκινά από 29,99 δολάρια ανά έτος (εκδοχή Personal, για οικιακά περιβάλλοντα ή για εκπαιδευτικούς σκοπούς — βλ. και https://www.snort.org/products). Αναφορικά τώρα με τη συχνότητα αυτόματης λήψης ενημερώσεων ανεξαρτήτως ruleset, η προκαθορισμένη τιμή είναι οι 12 ώρες (4). Μιλάμε δηλαδή για δύο ενημερώσεις μέσα στο 24ωρο και η πρώτη προτείνεται να ξεκινά πέντε λεπτά μετά τα μεσάνυχτα (5). Δεν ξέρουμε για εσάς, εμείς όμως είμαστε μια χαρά τόσο με τη συχνότητα, όσο και με την ώρα που ξεκινά η πρώτη ενημέρωση :)

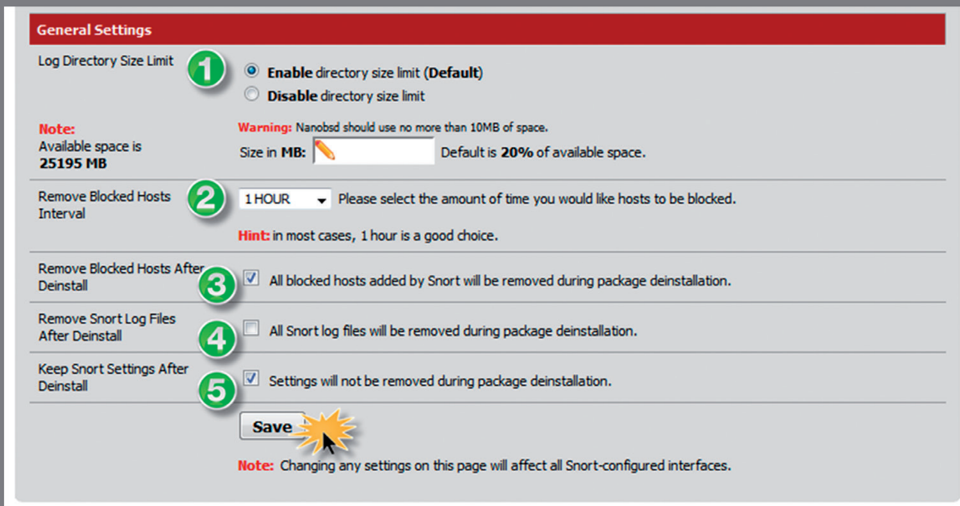


Το Snort καταγράφει μια υπερπληθώρα πληροφοριών που αφορούν στη δικτυακή κίνηση. Μιας και κατά πάσα πιθανότητα ο δίσκος του pfSense δεν είναι μεγάλος, είναι καλή ιδέα να θέσουμε ένα άνω όριο στο μέγεθος του καταλόγου με τα αρχεία καταγραφής. Ακριβώς γι' αυτό, φροντίστε ώστε να είναι επιλεγμένο το Enable directory size limit (1). Εξ ορισμού, το μέγιστο επιτρεπτό μέγεθος του εν λόγω καταλόγου είναι το 20% του διαθέσιμου αποθηκευτικού χώρου. Το Snort εξάλλου έχει την ικανότητα να μπλοκάρει hosts τα οποία σχετίζονται με ύποπτες ή με ξεκάθαρα κακόβουλες ενέργειες. Γενικά, παρέχει στο χρήστη μια επιλογή του στιλ "να μπλοκάρεται όποιο host προκαλεί alert" (βλ. συνέχεια). Προφανώς, τέτοια hosts καλό είναι να μην παραμένουν μπλοκαρισμένα για πάντα — υπάρχουν άλλωστε και οι περιπτώσεις των false positives! Θέλουμε, λοιπόν, τα hosts που μπλοκάρονται να ξεμπλοκάρονται μετά το πέρας χρόνου που εμείς έχουμε ορίσει. Το προτεινόμενο χρονικό διάστημα κατά το οποίο θα παραμένουν μπλοκαρισμένα τα "κακόβουλα" hosts, είναι η μία ώρα (βλ. παράμετρο Remove Blocked Hosts Interval, (2)). Φανταστείτε τώρα ότι για κάποιο λόγο χρειάζεται να απεγκαταστήσετε το Snort. Για μια τέτοια περίπτωση, ίσως αξίζει να σκεφτείτε από τώρα τα ακόλουθα:

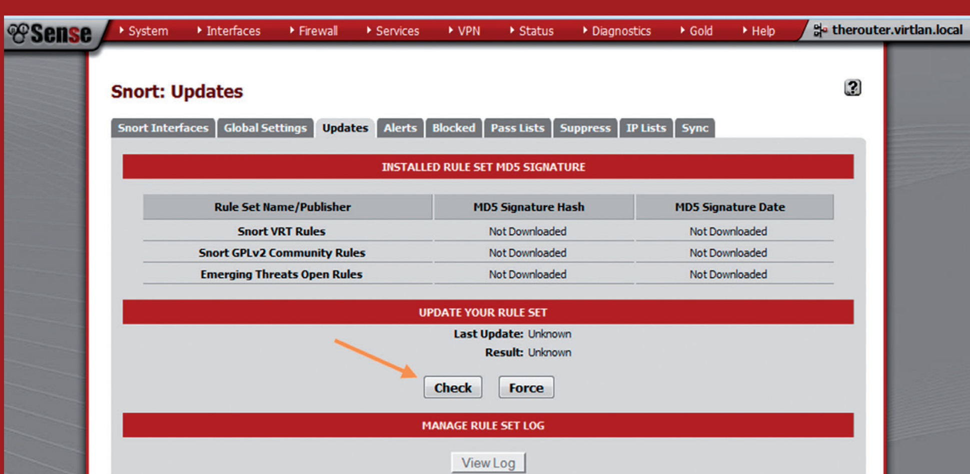
- Θέλετε το firewall του pfSense (το pf) να συνεχίσει να μπλοκάρει τα κακόβουλα hosts; (Remove Blocked Hosts After Deinstall, (3))
- Να διαγραφούν τα log files που έχει δημιουργήσει το Snort; (Remove Snort Log Files After Deinstall, (4))

- Να διατηρηθούν οι επιλογές σας, ώστε αν αργότερα εγκαταστήσετε ξανά το Snort να ληφθούν υπόψη αυτομάτως; (Keep Snort Settings After Deinstall, (5))

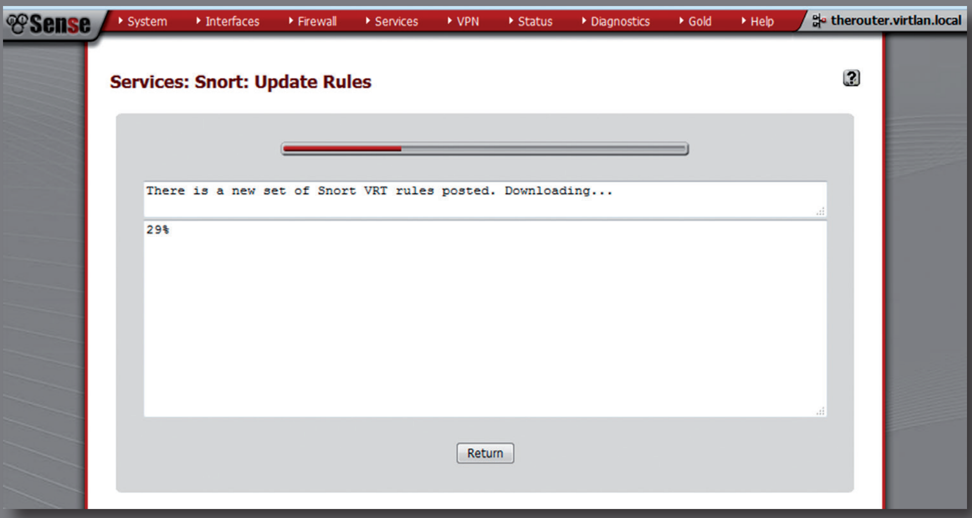
Σίγουρα ο καθένας δίνει διαφορετικές απαντήσεις σε τέτοια ερωτήματα — και οι δικές μας φαίνονται στο screenshot. Αφού τελειώσουμε με τις γενικές επιλογές και ρυθμίσεις, τις επικυρώνουμε μ' ένα κλικ στο [Save].



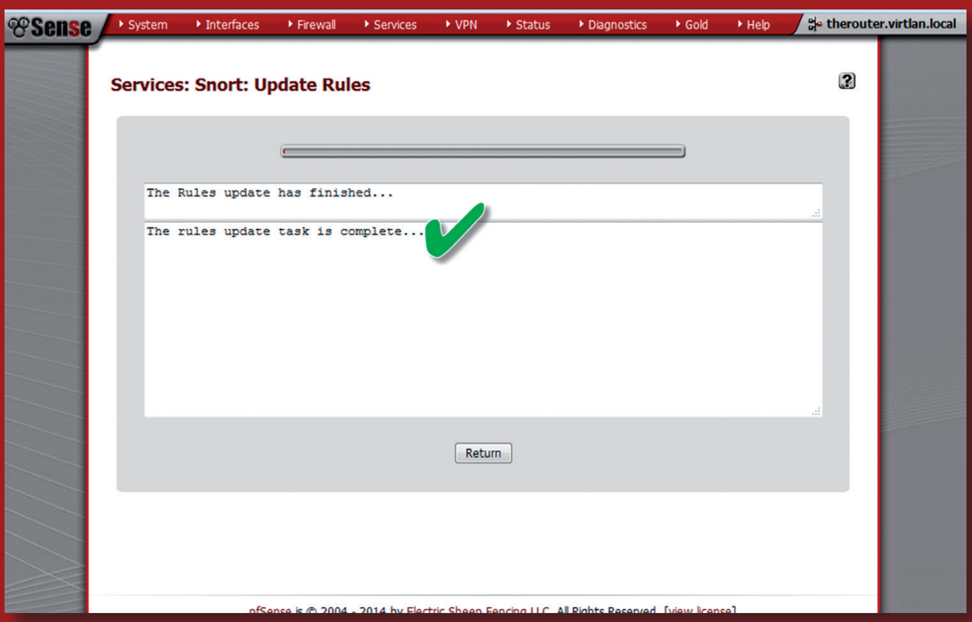
Η εγκατάστασή μας είναι φρέσκια και, απ' ό,τι βλέπουμε ακολουθώντας τη διαδρομή Services → Snort → Updates, δεν έχουμε ακόμη κανόνες για κάποιο από τα σύνολα VRT, Community και Emerging Threats Open (ETOpen). Κάνουμε λοιπόν ένα κλικ στο κουμπάκι [Check], ώστε να ελέγξουμε online για διαθέσιμα rulesets.



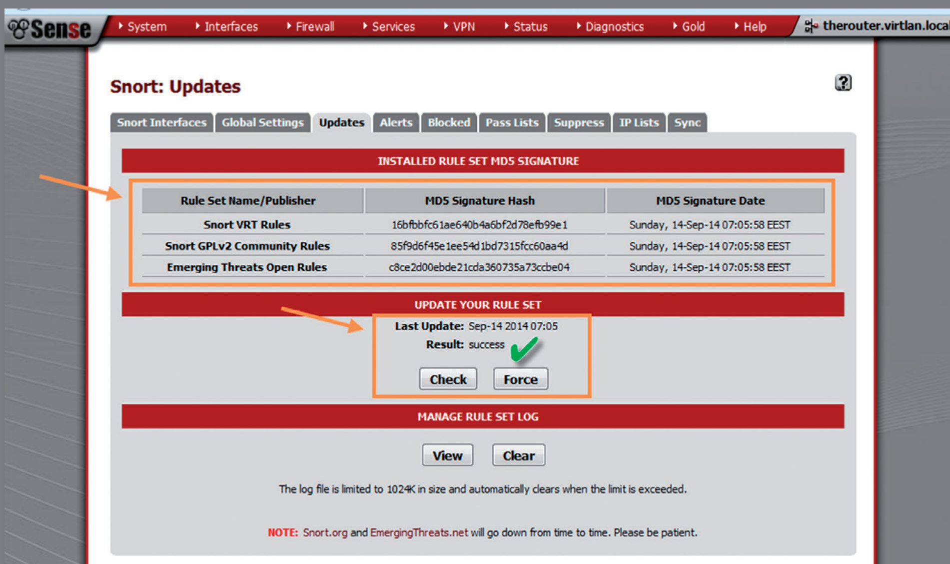
Όπως το αναμέναμε, rulesets υπάρχουν! (Κι εδώ ο γράφων κάνει γενναία προσπάθεια προκειμένου ν' αποφύγει το σχεδόν αυτόματο αστείο που ήδη όλοι ακούσαμε με τη φαντασία μας.) Στο στιγμιότυπο βλέπουμε την πρόοδο λήψης των VRT rules.



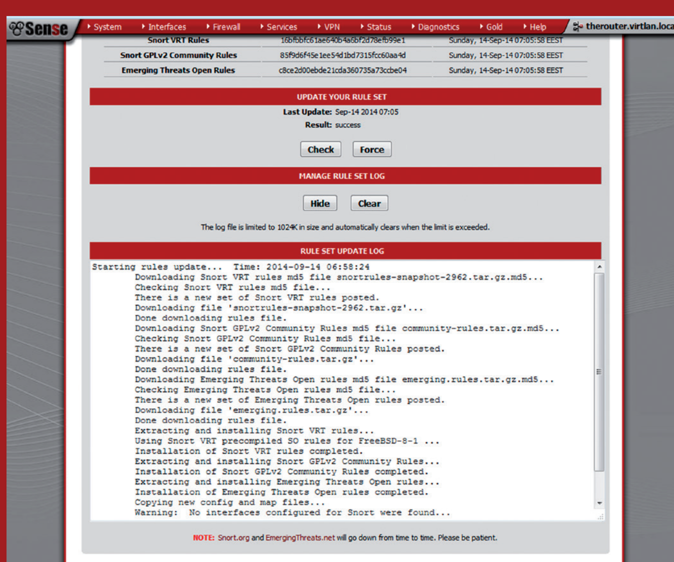
Αναλόγως της ταχύτητας σύνδεσης, ειδικά την πρώτη φορά η διαδικασία λήψης ενδέχεται να χρειαστεί αρκετά λεπτά για να ολοκληρωθεί. Αλλά βεβαίως κάποια στιγμή θα ολοκληρωθεί, κι εμείς θα ενημερωθούμε με σχετικό μήνυμα.



Για τα rulesets που κατεβάζουμε υπολογίζονται τα MD5 hashes, ενώ παρατίθενται και οι αντίστοιχες ημερομηνίες και ώρες. Αυτές οι πληροφορίες είναι χρήσιμες για όσους θέλουν να ελέγξουν τα hashes με εκείνα που δίνονται από τον επίσημο δικτυακό τόπο του Snort.



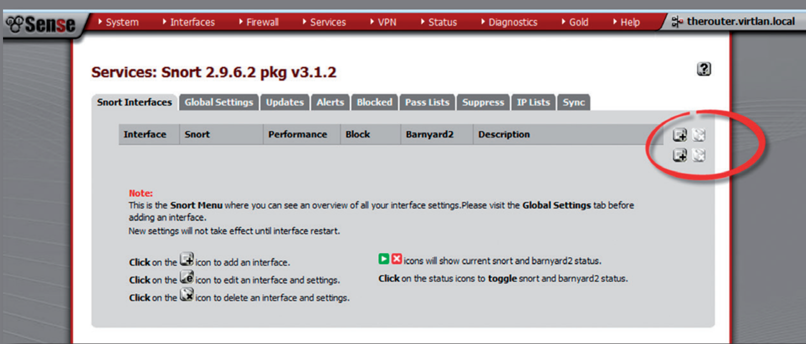
Λίγο να μας μοιάζετε, και στην ενότητα MANAGE RULE SET LOG οπωσδήποτε θα πατήσετε το κουμπάκι [View], από κάτω. Αμέσως θα εμφανιστεί ένα χρήσιμο —και καθόλου φλύαρο— αρχείο καταγραφής, με τα πλέον πρόσφατα ruleset updates.



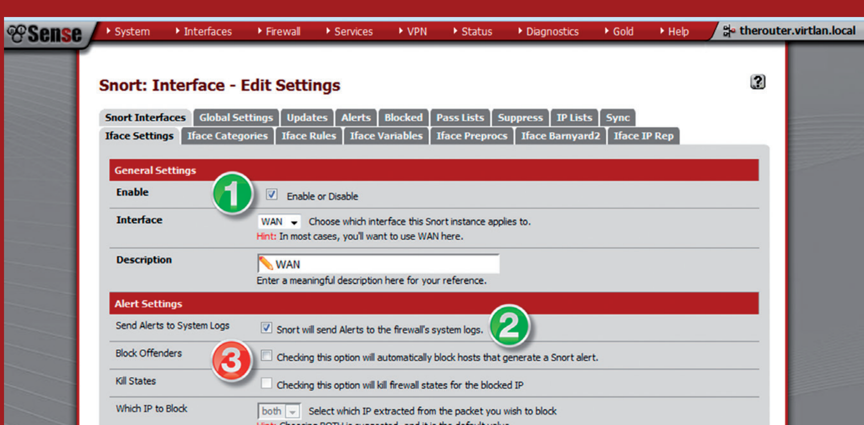
Καθορισμός των Snort interfaces

Όπως είπαμε και πριν λίγο, το Snort παρακολουθεί τη δικτυακή κίνηση από τουλάχιστον ένα network interface. Σε διαφορετική περίπτωση δεν θα μπορούσε να γνωρίζει τίποτε για το τι συμβαίνει στο δίκτυο — πόσο μάλλον να παίρνει αποφάσεις, π.χ., για το αν πρέπει να μπλοκάρει κάποιο host ή όχι. Για αρχή, λοιπόν, ας το βάλουμε να ελέγχει τα πακέτα που φτάνουν στο WAN από τον έξω κόσμο.

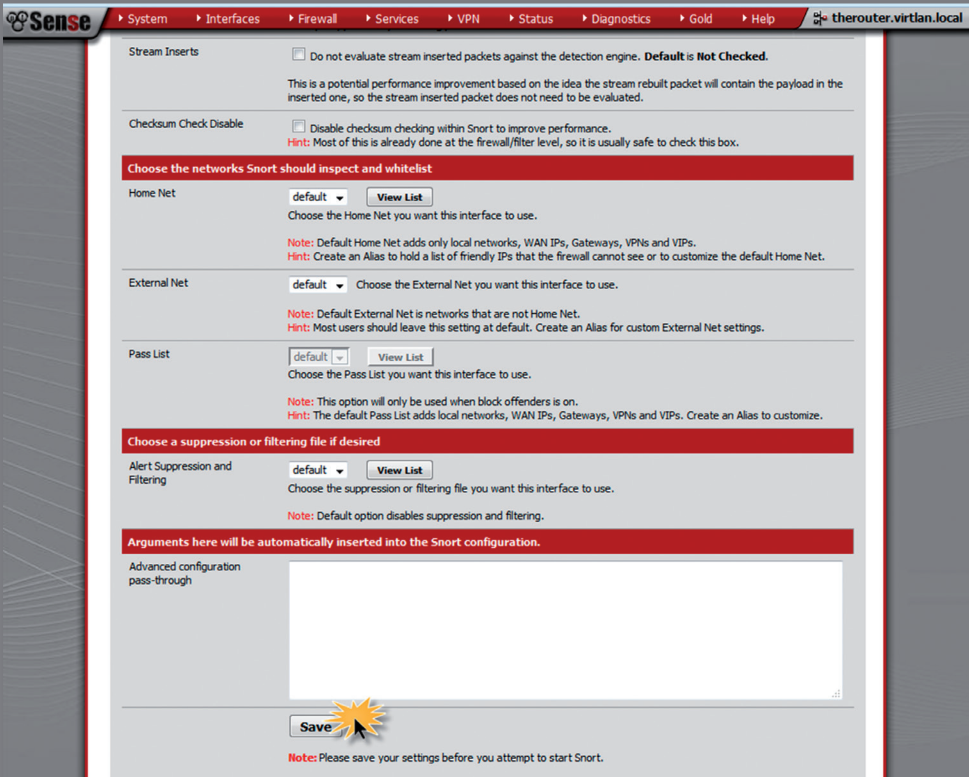
Στο web panel του pfSense δίνουμε Services → Snort → Snort Interfaces. Λογικά, δεν θα υπάρχει κανένα network interface του συστήματος στη λίστα. Κάνουμε λοιπόν κλικ σε κάποιο από τα δύο κουμπάκια [+], στα δεξιά.



Στην καρτέλα Iface Settings (αριστερά) φροντίζουμε ώστε το κουτάκι Enable or Disable να είναι τσεκαρισμένο (1) κι από τη γραμμή Interface, από κάτω, επιλέγουμε το WAN: Είναι το δικτυακό ενδιάμεσο που στη σούπερ-συντριπτική πλειονότητα των περιπτώσεων χρησιμοποιεί το pfSense για να βγαίνει στον έξω κόσμο. Είναι καλή ιδέα να γράψουμε κάτι χαρακτηριστικό στη θυρίδα Description, από κάτω. Κάθε φορά εξάλλου που έχουμε alert καλό είναι να αντικατοπτρίζεται και στα logs του firewall, δηλαδή στα logs του pf (2). Έως ότου αποκτήσουμε μια καλή αίσθηση του πώς δουλεύει το Snort, τα hosts που προκαλούν alerts ας μην μπλοκάρονται. Ακριβώς γι' αυτό, εμείς τουλάχιστον προτείνουμε να μην τσεκάρετε το κουτάκι Block Offenders (3).

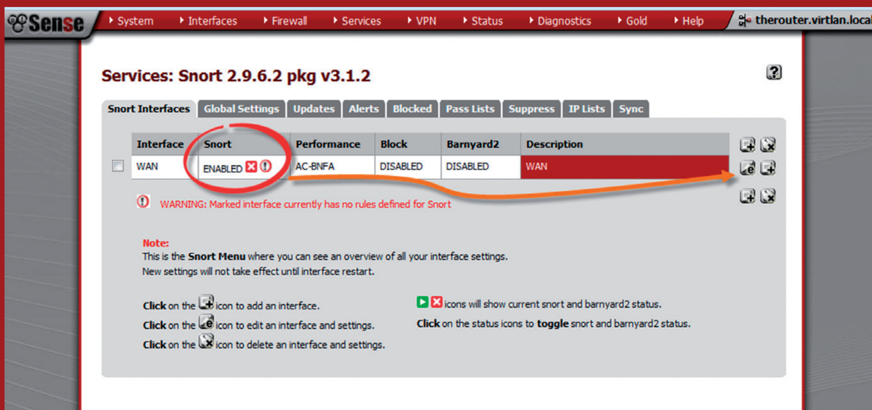


Δεν πειράζουμε κάποια άλλη επιλογή της καρτέλας Iface Settings. Απλά πηγαίνουμε στο κάτω μέρος της σελίδας και πατάμε στο [Save].





Πίσω στην καρτέλα Snort Interfaces, παρατηρούμε ότι ναι μεν το Snort είναι ενεργοποιημένο για το WAN interface που μόλις του υποδείξαμε, αλλά δεν έχουν ακόμα οριστεί σχετικοί κανόνες (WARNING: Marked interface currently has no rules defined for Snort). Δεν υπάρχει πρόβλημα: Κάνουμε ένα κλικ στο κουμπάκι [e], στα δεξιά της γραμμής.

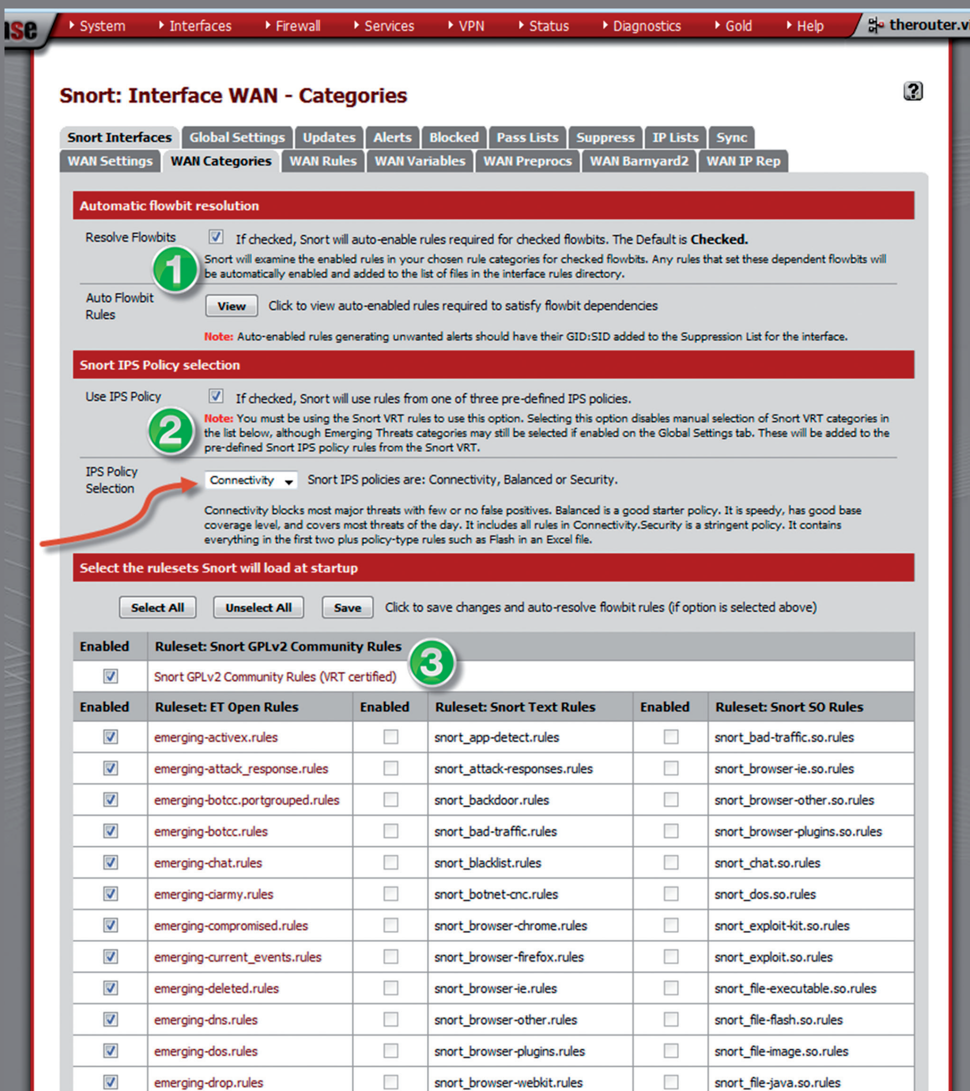


Πηγαίνουμε στην καρτέλα WAN Categories κι αρχικά φροντίζουμε ώστε το κουτάκι Resolve Flowbits να 'ναι τσεκαρισμένο (1). Τώρα, ασχέτως αν προηγουμένως επιλέξαμε να μη μπλοκάρονται τα hosts που προκαλούν alerts, αυτή τη στιγμή είναι καλό να επιλέξουμε μια πολιτική IPS. Αν δεν το κάνουμε, τότε θα υποχρεωθούμε να ενεργοποιήσουμε χειροκίνητα κανόνες από ένα σύνολο εκατοντάδων — κι αυτόν το μπελά κανείς εχέφρων χρήστης δεν τον θέλει. Τσεκάρουμε, λοιπόν, το κουτάκι Use IPS Policy (2). Υπάρχουν τρεις προκαθορισμένες πολιτικές IPS: η Connectivity, η Balanced και η Security.

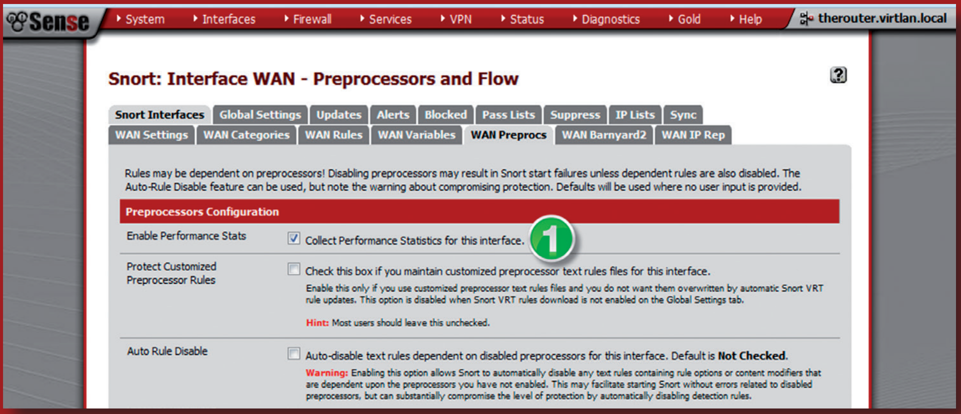
- Η Connectivity είναι η πιο χαλαρή, ανιχνεύει τις περισσότερες βασικές απειλές και παράγει ελάχιστα —αν όχι καθόλου— false positives.
- Η δε Balanced ουσιαστικά αποτελεί ένα υπερσύνολο κανόνων της Connectivity, ανιχνεύει περισσότερες απειλές αλλά παράγει και false positives.
- Τέλος, η Security είναι η πλέον αυστηρή πολιτική IPS, αφού εμπεριέχει όλους τους κανόνες των δύο προηγουμένων καθώς και κανόνες του στιλ "αυτό το αρχείο Excel είναι ύποπτο επειδή έχει ενσωματωμένο βίντεο flash".

Αν και προτείνεται να ξεκινήσετε με την πολιτική Balanced, σίγουρα δεν βλάπτει αν επιλέξετε την Connectivity. Όπως και να 'χει, κάντε την επιλογή σας στο drop-down μενού ονόματι IPS Policy Selection. Παρατηρήστε ότι, αν και μόλις επιλέξαμε πολιτική IPS, εξακολουθούμε να 'χουμε δυνατότητα επιλογής κανόνων που θα φορτώνονται κατά την ενεργοποίηση του Snort για το συγκριμένο interface (βλ. περιοχή "Select the rulesets Snort will load at startup"). Κατ' αρχάς, ας επιλέξουμε τους κανόνες από τη συλλογή Community (3). Από κάτω υπάρχει επίσης και η συλλογή ETOpen, η οποία απαρτίζεται από διάφορα υποσύνολα κανόνων. Αν θέλετε, επιλέξτε τα όλα μ' ένα κλικ στο κουμπάκι [Select All]. Προσέξτε ότι για

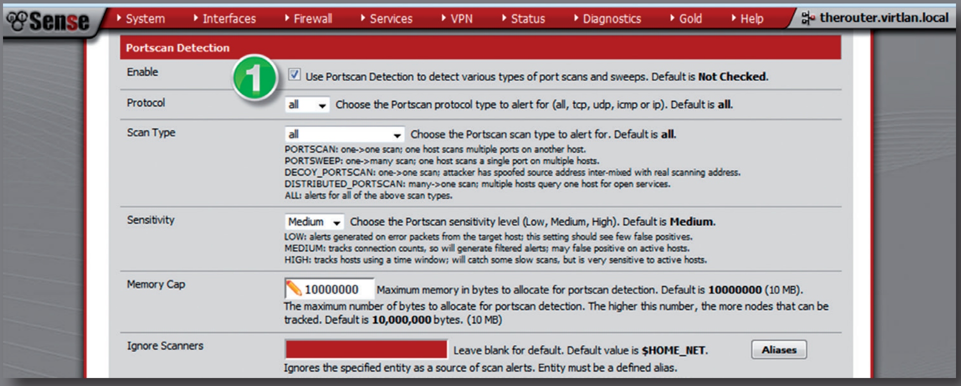
τα σύνολα "Snort Text Rules" και "Snort SO Rules" (βλ. μεσαία και δεξιά στήλη) δεν παρέχεται δυνατότητα επιλογής υποσυνόλων κανόνων. Αυτό συμβαίνει διότι έχουμε ήδη καθορίσει πολιτική IPS. Αν δεν είχαμε, τώρα θα πελαγώναμε χαρούμενα κι ωραία. Αλλά αφού προφανώς και δεν πελαγώνουμε (χαρούμενα κι ωραία), αρκούμαστε σ' ένα κλικ στο κουμπάκι [Save].



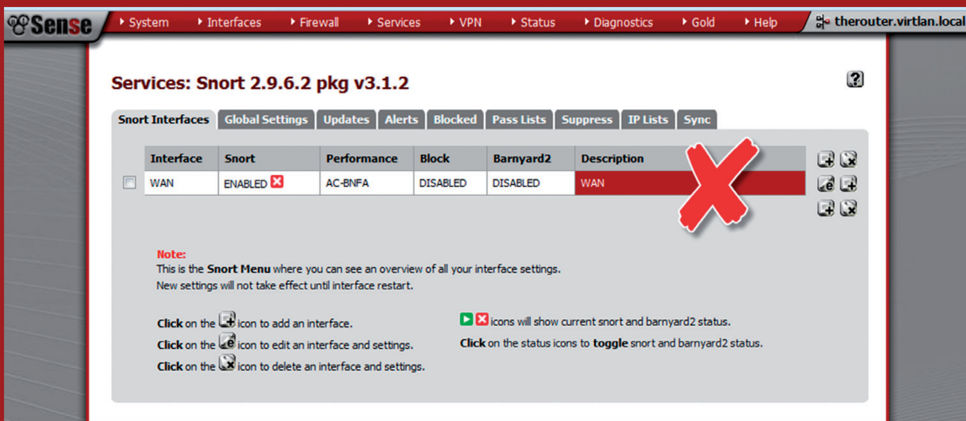
Πηγαίνουμε στην καρτέλα WAN Preprocs και φροντίζουμε ώστε το κουτάκι Collect Performance Statistics for this interface (1) να 'ναι τσεκαρισμένο.



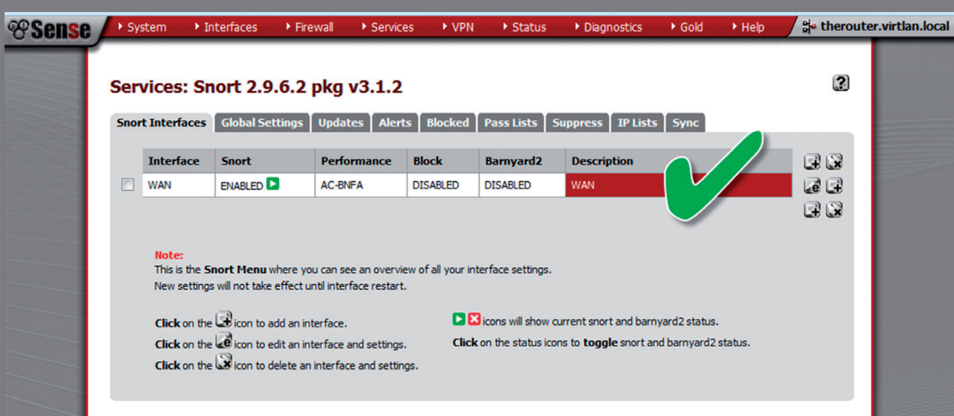
Πιο κάτω στην ίδια καρτέλα —και συγκεκριμένα στην ενότητα Portscan Detection— ενεργοποιούμε τη δυνατότητα ανίχνευσης αποπειρών για port scanning. Μετακινούμαστε στο κάτω μέρος της σελίδας και κάνουμε ένα κλικ στο [Save].



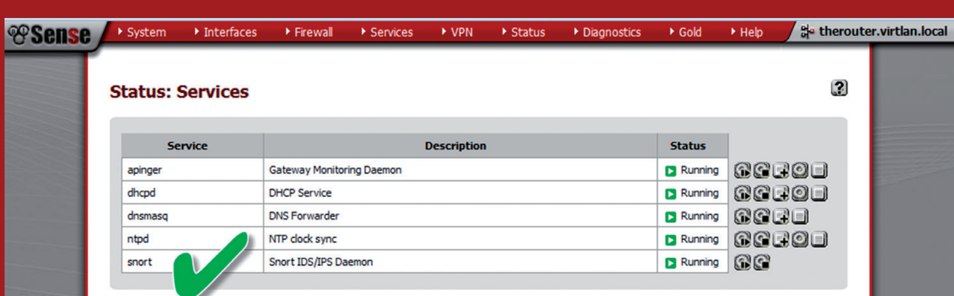
Στην καρτέλα Snort Interfaces βλέπουμε τώρα ότι έχει φύγει αυτό το θαυμαστικό και δεν υπάρχει κάποια προειδοποίηση. Δίπλα από το ENABLED όμως εξακολουθεί να υπάρχει ένα κόκκινο "x", που σημαίνει ότι το Snort δεν έχει ακόμα ενεργοποιηθεί για το WAN interface. Μα, τι θέλει επιτέλους για να ξεκινήσει;



Αυτό που θέλει είναι ένα κλικ πάνω στο κόκκινο "x" — κι αυτό αρκεί για να πάρει μπρος (so to speak).



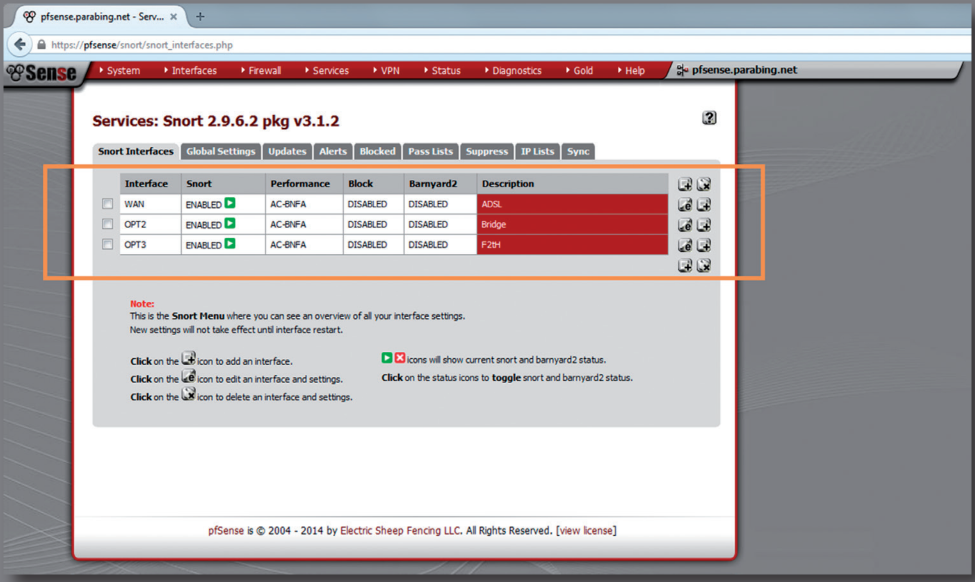
Δίνοντας Status → Services βλέπουμε όλες τις ενεργές υπηρεσίες του pfSense μας — και μεταξύ αυτών είναι κι εκείνη του Snort.

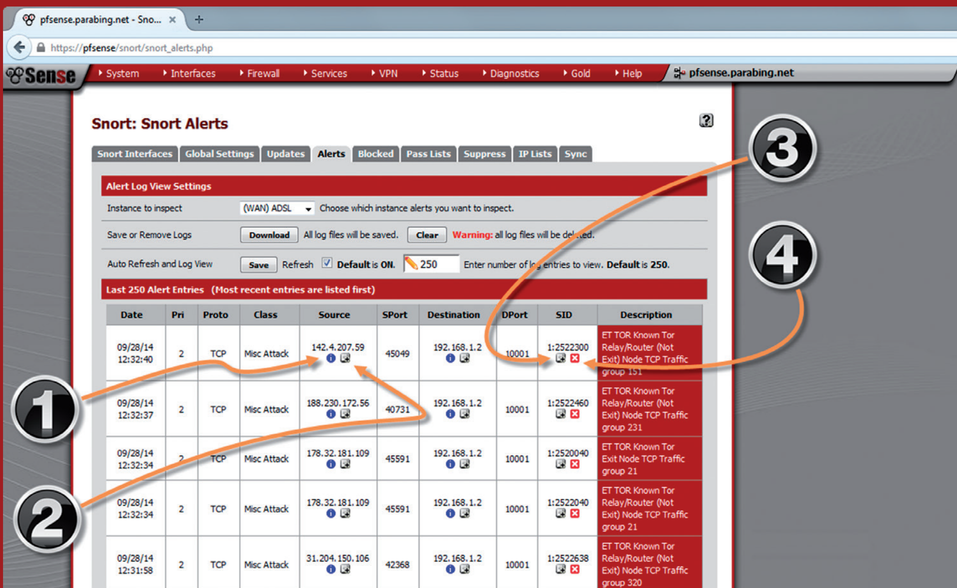


Το Snort εν δράσει!

Στα screenshots που ακολουθούν δείχνουμε μερικές όψεις της δικής μας εγκατάστασης του Snort, στο pfSense box που έχουμε στο δίκτυο της Parabing Creations (στο Northern Outpost του SKG, φυσικά :D). Πριν τα δείτε και διαβάσετε τις αντίστοιχες περιγραφές, θα θέλαμε να σημειώσουμε ότι όσα συζητάμε και παρουσιάζουμε στο παρόν άρθρο αποτελούν μια πρώτη μόνο εισαγωγή στο Snort αλλά και στον κόσμο του intrusion detection/prevention γενικότερα. Αν αποφασίσετε ν' ασχοληθείτε στην πράξη πιστεύουμε ότι θα πάρετε μια πολύ καλή ιδέα για τις ικανότητες και τη χρησιμότητα των σχετικών συστημάτων. Θεωρούμε εξάλλου ότι η εκτίμηση ενός νεοφερμένου απέναντι σε κάποιο IDS αυξάνει σημαντικά και γρήγορα, αρκεί να έχει πρόσβαση σε κάποιο βολικό, εύχρηστο —γιατί όχι κι όμορφο— μέσο παρουσίασης των alerts που παράγει το εκάστοτε IDS. Υπάρχουν διάφορα προγράμματα με αποστολή τη συγκέντρωση, ομαδοποίηση κι οπτικοποίηση των alerts συστημάτων IDS (βλ., π.χ., `http://blog.snort.org/2011/01/guis-for-snort.html`). Στο site του περιοδικού, συγκεκριμένα στη σελίδα `http://deltahacker.gr/?p=12305`, μπορείτε να διαβάσετε για τη συνεργασία Snort (στο pfSense) με το Snorby (στο Security Onion). Μεταξύ άλλων θα δείτε και τι είναι αυτό το Barnyard, που τόση ώρα βλέπαμε στο web panel του pfSense αλλά (αμήχανα) αποφεύγαμε ν' αναφέρουμε.

Στο δικό μας pfSense box το Snort επιβλέπει τρία διαφορετικά network interfaces. Τα WAN και OPT3 αντιστοιχούν σε δύο διαφορετικές συνδέσεις προς το Internet, μία ADSL και μία fiber. Για τα δύο αυτά interfaces έχουμε φτιάξει δύο gateway groups που χρησιμοποιούμε κατά περίπτωση: το ένα είναι σε διάταξη load balancing και το άλλο σε διάταξη fail-over. Δείτε το άρθρο που αρχίζει από τη σελίδα 50 του deltaHacker 029 για όλες τις λεπτομέρειες. Το δε OPT2 είναι ένα bridge για το εσωτερικό δίκτυο, πίσω από τον router. Περί bridging μπορείτε να διαβάσετε στο άρθρο που αρχίζει από τη σελίδα 24 του deltaHacker 027.





Δίνοντας Services → Snort → Alerts βλέπουμε τις ειδοποιήσεις (alerts) που παράγει το Snort για κάθε network interface που επιβλέπει. Στην εικόνα φαίνεται ένα ελάχιστο μέρος των ουκ ολίγων alerts που αφορούν στο WAN interface — και να φανταστείτε ότι κατά κύριο λόγο χρησιμοποιούμε το OPT3. Γιατί, λοιπόν, τόσα πολλά alerts για το WAN; Πολύ απλά, διότι σ' ένα Raspberry Pi του τοπικού δικτύου τρέχουμε ένα Tor relay (με όνομα "thessaloniki", βλ. http://bit.ly/skgrelay) και στους κανόνες του firewall υπάρχει ένας που υποχρεώνει το συγκεκριμένο Raspberry Pi να έχει ως gateway το WAN interface. Την ίδια στιγμή, το Snort έχει φορτωμένους κανόνες που είναι κάπως ευαίσθητοι ως προς τα Tor relays, εξ ου κι όλες αυτές οι αναφορές. Σημειώστε εδώ ότι αν είχαμε ζητήσει από το Snort να μπλοκάρει αυτόματα τα hosts που παράγουν alerts, τότε το Tor relay μας δεν θα συνεισέφερε και πολλά στο αντίστοιχο δίκτυο ανωνυμίας. Αλλά ακόμη και τώρα, που το Snort δεν μπλοκάρει τα "offending" hosts, από τη στιγμή που έχουμε μια καλή ιδέα για το τι γίνεται στο δίκτυό μας είναι πολύ πιθανό ότι δεν θα θέλουμε να παράγονται alerts που για εμάς αποτελούν false positives και τίποτε περισσότερο. Δείτε, λοιπόν, πώς βάζουμε τάξη στις αναφορές του Snort, ουσιαστικά προσαρμόζοντάς το στο δίκτυό μας.

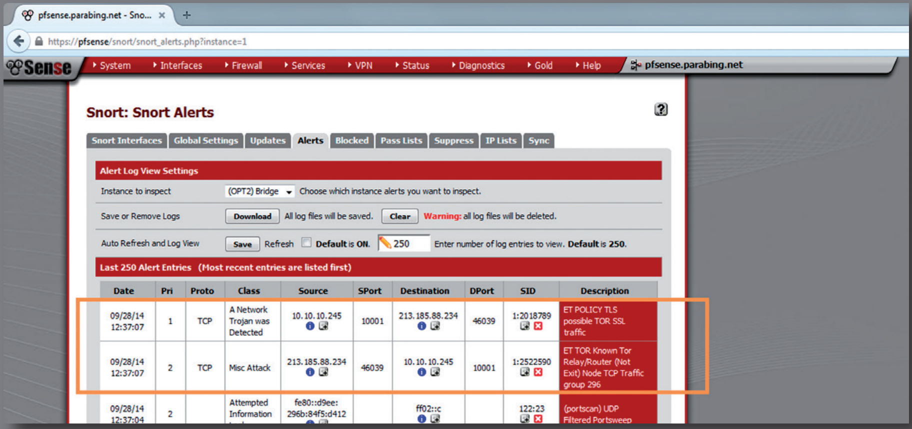
(1) Με κλικ στο μπλε εικονίδιο γίνεται reverse DNS lookup στο αντίστοιχο IP. Αυτό είναι αρκετές φορές χρήσιμο, ώστε, π.χ., να βλέπουμε στα γρήγορα αν το host έχει κάποια δουλειά να επικοινωνεί με τον router μας. Ένα παράδειγμα από την εγκατάστασή μας: Κάνοντας rDNS lookup στο 194.158.67.136 πήραμε το host με όνομα static-194-158-67-136.andorpac.ad και το ".ad" είναι το top-level domain της Ανδόρρας. Συνεπώς, το αντίστοιχο alert ("ET CINS Active Threat Intelligence Poor Reputation IP TCP group 22") δεν ήταν false positive κι αν είχαμε ενεργοποιημένο το blocking καθόλου δεν θα μας πείραζε ο αποκλεισμός του Ανδορρανού (;) host. Μερικές φορές πάντως το rDNS lookup δεν επιστρέφει κάποιο όνομα, αφού

πολύ απλά δεν υπάρχει. Από το αντίστοιχο alert, όμως, φαίνεται αμέσως αν πρόκειται για false positive ή όχι. Όταν, π.χ., βλέπεις το host με IP το 58.221.114.25 να προσπαθεί να συνδεθεί στο port 3306 της MySQL και δεν έχεις κάποιον MySQL server "ανοιχτό" στο Internet, ε, τότε ξέρεις ότι το απομακρυσμένο μηχάνημα είναι κακόβουλο και το alert με περιγραφή "ET POLICY Suspicious inbound to mySQL port 3306" είναι πέρα για πέρα έγκυρο.

(2) Μερικές φορές δεν θέλουμε να παράγονται alerts συγκεκριμένου τύπου για συγκεκριμένα hosts, οπότε κάνουμε ένα κλικ στο κουμπάκι [+], κάτω από το IP του host που επιθυμούμε να απεμπλέξουμε. Το IP του host μπαίνει τότε σε ένα κατάλληλο suppress list —πηγαίνετε στην καρτέλα Suppress για να δείτε όλες αυτές τις λίστες, αν υπάρχουν—, και πλέον δεν παίρνουμε alerts σαν αυτό που μόλις αποσιωπήσαμε. Εννοείται επίσης ότι το εμπλεκόμενο host δεν πρόκειται να μπλοκαριστεί, ακόμη κι αν ενεργοποιήσουμε το "Block Offenders" για το αντίστοιχο interface. Προσέξτε, όμως: Ο κανόνας που παρήγαγε το αποσιωπημένο, πλέον, alert, παραμένει ενεργός και συνεχίζει να παράγει παρόμοια alerts για *άλλα* hosts, τα οποία ίσως να μπλοκάρονται κιόλας (αρκεί να 'ναι ενεργοποιημένο το "Block Offenders").

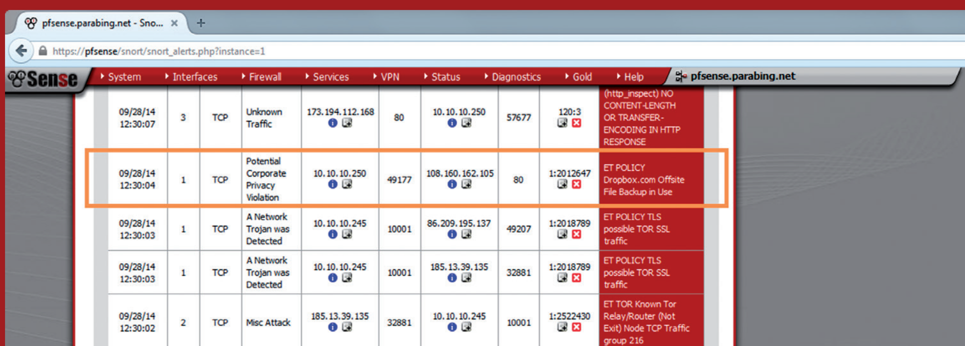
(3) Υπάρχουν περιπτώσεις όπου θα θέλουμε να αδρανοποιούμε συγκεκριμένους κανόνες, ώστε ναι μεν να μην παράγουν alerts για κανένα host αλλά ταυτόχρονα να μην απενεργοποιούνται για το συγκεκριμένο network interface. Προς τούτο, ένα κλικ στο κουμπάκι [+] της στήλης SID (Signature ID) για την αντίστοιχη γραμμή (κανόνας) θα είναι αρκετό.

(4) Βεβαίως, παρατηρώντας τη συμπεριφορά του Snort κι ενδεχομένως τις επιπτώσεις που έχουν τα alerts που παράγει, συχνά θα θέλουμε να απενεργοποιούμε —όχι απλά να αδρανοποιούμε— συγκεκριμένους κανόνες. Θα πηγαίνουμε τότε στη στήλη SID και θα κάνουμε κλικ στο κόκκινο κουμπάκι [x]. Μετά από λίγο, το κόκκινο [x] ενός απενεργοποιημένου κανόνα θα κιτρινίζει. Δεν είναι διόλου απίθανο να επιθυμούμε και την απενεργοποίηση όλων των κανόνων ενός ολόκληρου ruleset. Εμείς, π.χ., για το WAN interface απενεργοποιούμε το ruleset ονόματι "emerging-tor.rules": Services → Snort → Snort Interfaces → WAN → [e] → WAN Categories, αποεπιλογή του "emerging-tor.rules", κλικ στο [Save].



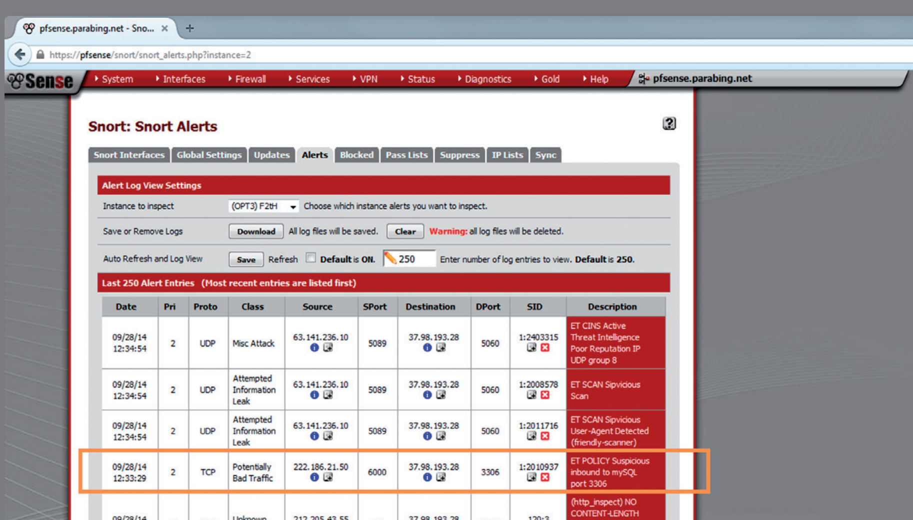
Εδώ βλέπουμε το bridge interface (OPT2), το οποίο αφορά στο εσωτερικό δίκτυο, πίσω από τον router. Το μηχάνημα με IP το 10.10.10.245 είναι εκείνο το Raspberry Pi και το Snort θορυβείται στην πιθανότητα το κρυπτογραφημένο traffic που ξεκινά ή καταλήγει στο Pi να 'χει σχέση με το Tor. Εμείς βέβαια ξέρουμε ποιος είναι ο ρόλος του Pi, οπότε αγνοούμε τα σχετικά alerts.

Να κι ένα alert για μηχάνημα του τοπικού δικτύου. Η ειδοποίηση οφείλεται σε κανόνα ο οποίος είναι αυτό που θα λέγαμε "policy-related": Γίνεται χρήση του Dropbox — κι αυτό γενικά δεν είναι πάντα επιθυμητό, σε κάθε δίκτυο. Στο δικό μας, όμως, είναι.



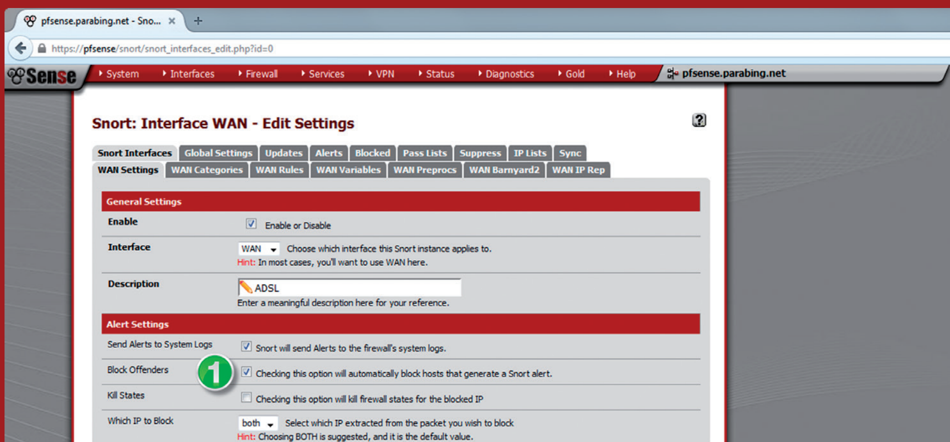
09/28/14 12:30:07	3	TCP	Unknown Traffic	173.194.112.168	80	10.10.10.250	57677	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
09/28/14 12:30:04	1	TCP	Potential Corporate Privacy Violation	10.10.10.250	49177	108.160.162.105	80	1:2012647	ET POLICY Dropbox.com Offsite File Backup in Use
09/28/14 12:30:03	1	TCP	A Network Trojan was Detected	10.10.10.245	10001	86.209.195.137	49207	1:2018789	ET POLICY TLS possible TOR SSL traffic
09/28/14 12:30:03	1	TCP	A Network Trojan was Detected	10.10.10.245	10001	185.13.39.135	32881	1:2018789	ET POLICY TLS possible TOR SSL traffic
09/28/14 12:30:02	2	TCP	Misc Attack	185.13.39.135	32881	10.10.10.245	10001	1:2522430	ET TOR Known Tor Relay/Router (Not Exit) Node TCP Traffic group 216

Στεκόμαστε τώρα για λίγο και στο OPT3 network interface, το οποίο αντιστοιχεί, ουσιαστικά, στη σύνδεση fiber που έχουμε εδώ, στο γραφείο. Το πλαισιωμένο alert προειδοποιεί για ανεπιθύμητη απόπειρα σύνδεσης στο τυπικό TCP port που χρησιμοποιεί ένας MySQL server. Το απομακρυσμένο host, με IP το 222.186.21.50, είναι από αυτά που καθόλου δεν θα μας ενοχλούσε αν μπλοκαριζόταν.

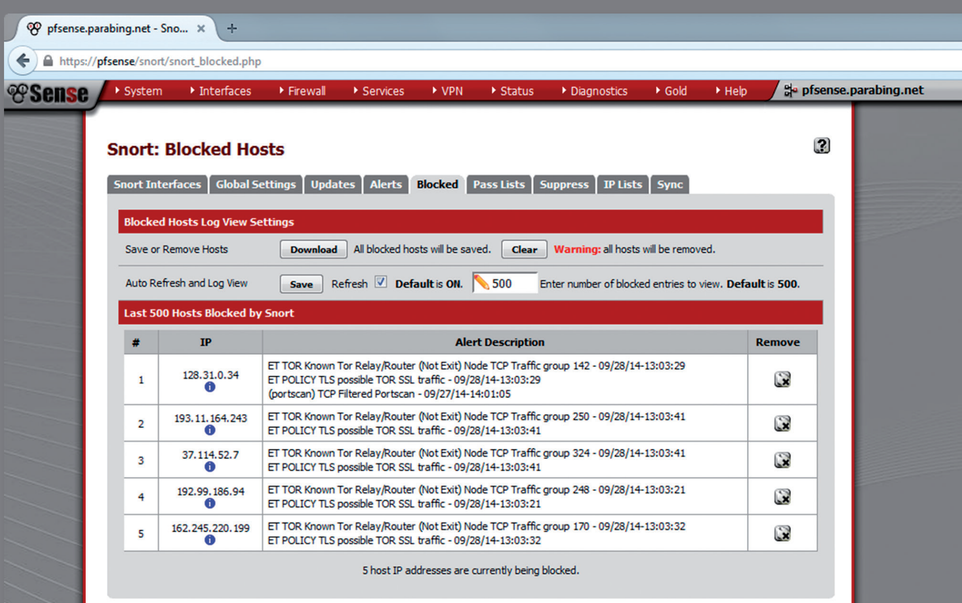


Date	Pri	Proto	Class	Source	SPort	Destination	DPort	SID	Description
09/28/14 12:34:54	2	UDP	Misc Attack	63.141.236.10	5089	37.98.193.28	5060	1:2403315	ET CINS Active Threat Intelligence Poor Reputation IP UDP group 8
09/28/14 12:34:54	2	UDP	Attempted Information Leak	63.141.236.10	5089	37.98.193.28	5060	1:2008578	ET SCAN Sipvicious Scan
09/28/14 12:34:54	2	UDP	Attempted Information Leak	63.141.236.10	5089	37.98.193.28	5060	1:2011716	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)
09/28/14 12:33:29	2	TCP	Potentially Bad Traffic	222.186.21.50	6000	37.98.193.28	3306	1:2010937	ET POLICY Suspicious inbound to mySQL port 3306
09/28/14	3	TCP	Unknown	212.205.43.55	80	37.98.193.28	13509	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-

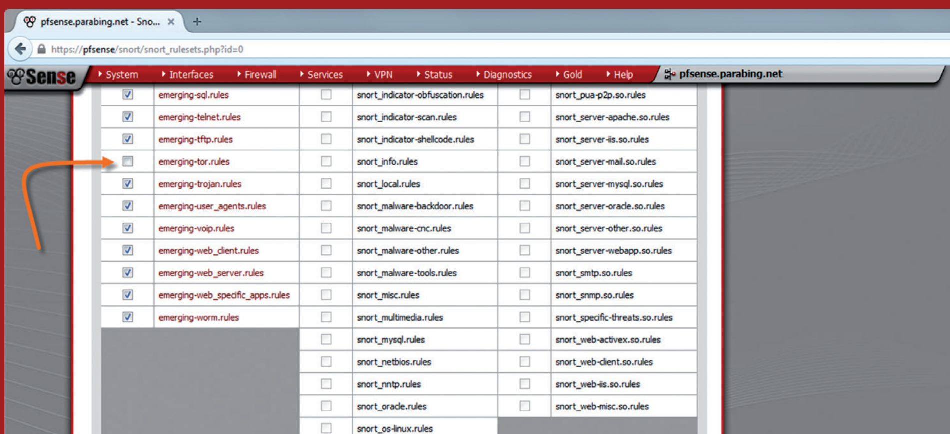
Πάμε και πάλι στο WAN interface και συγκεκριμένα στις αντίστοιχες ρυθμίσεις του Snort. Δεν είχαμε ζητήσει να μπλοκάρονται τα hosts που προκαλούν alert, τώρα όμως λέμε να το αλλάξουμε αυτό (1). Προσοχή: Την επιλογή για μπλοκάρισμα ή όχι των offending hosts πρέπει να ακολουθεί επανεκκίνηση του Snort για το αντίστοιχο network interface.



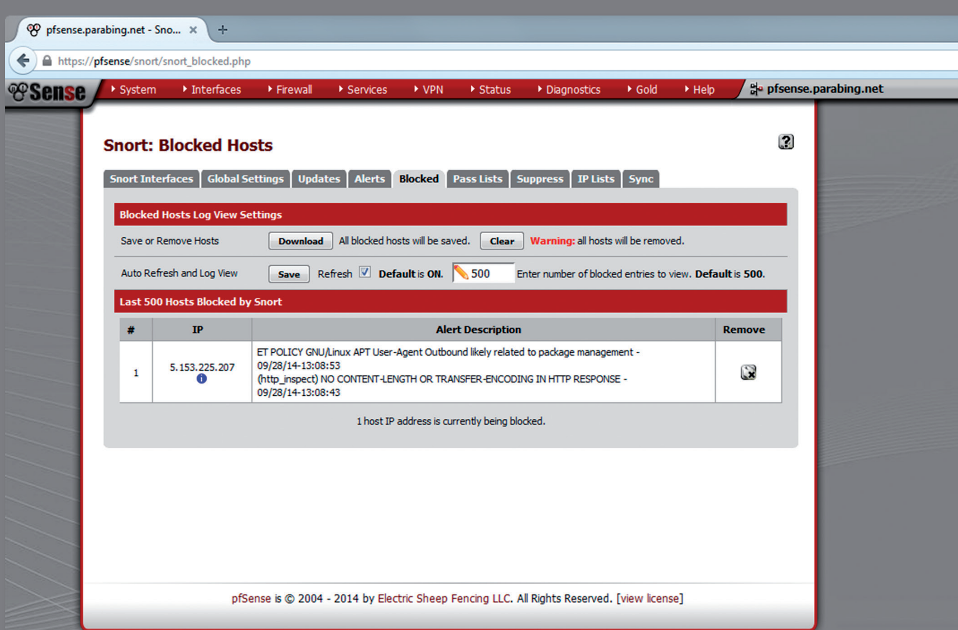
Αμέσως αμέσως, πέντε remote hosts μπλοκάρονται. Υπεύθυνοι για τον αποκλεισμό τους είναι το Raspberry Pi, που βγαίνει στο Internet μέσω του WAN interface, καθώς κι εκείνοι οι κανόνες του Snort που αφορούν στα Tor relays.



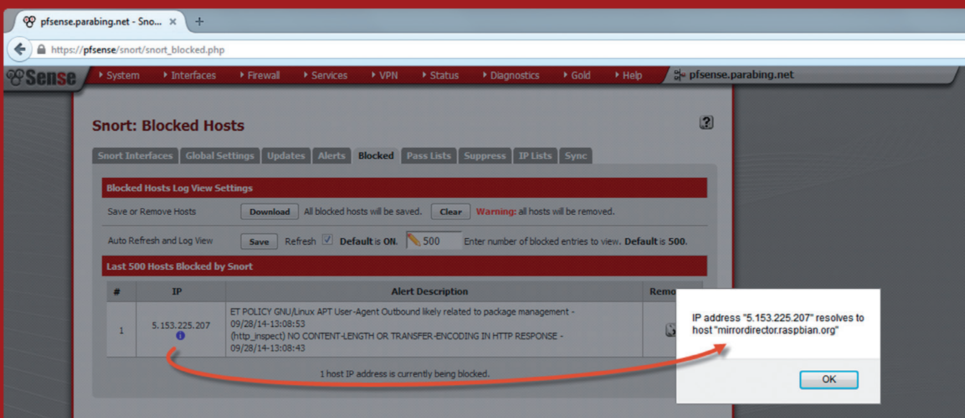
Ένα host που έχει μπλοκαριστεί μπορούμε εύκολα να το ξεμπλοκάρουμε, με κλικ στο αντίστοιχο κουμπάκι [x] (βλ. καρτέλα "Blocked"). Βέβαια, σε κάποιες περιπτώσεις δεν έχει νόημα να ξεμπλοκάρουμε μεμονωμένα hosts αλλά να απενεργοποιούμε τους κανόνες που οδήγησαν στο μπλοκάρισμά τους in the first place. (Sorry γι' αυτό, στάθηκε αδύνατο να του αντισταθούμε.)



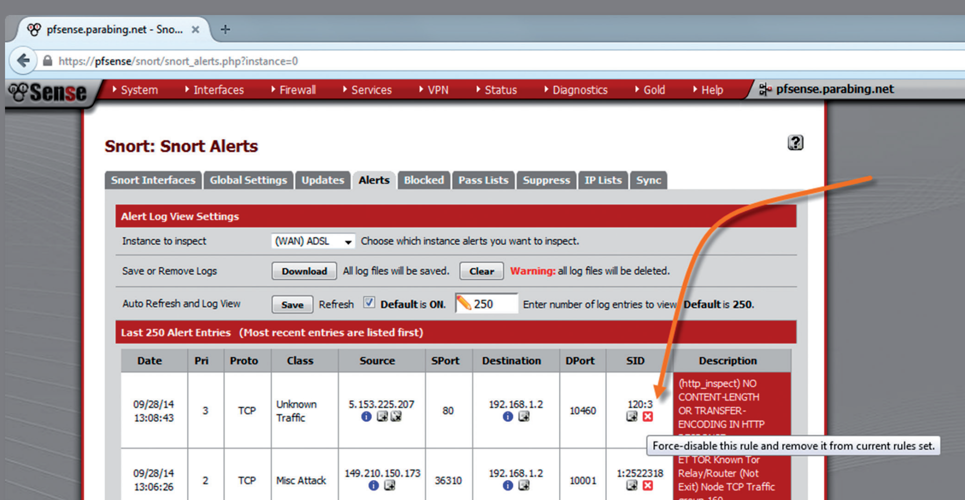
Χμ. Να κι ένα host που μπλοκαρίστηκε εξαιτίας ενός κανόνα που δεν είχαμε προσέξει ως τώρα.



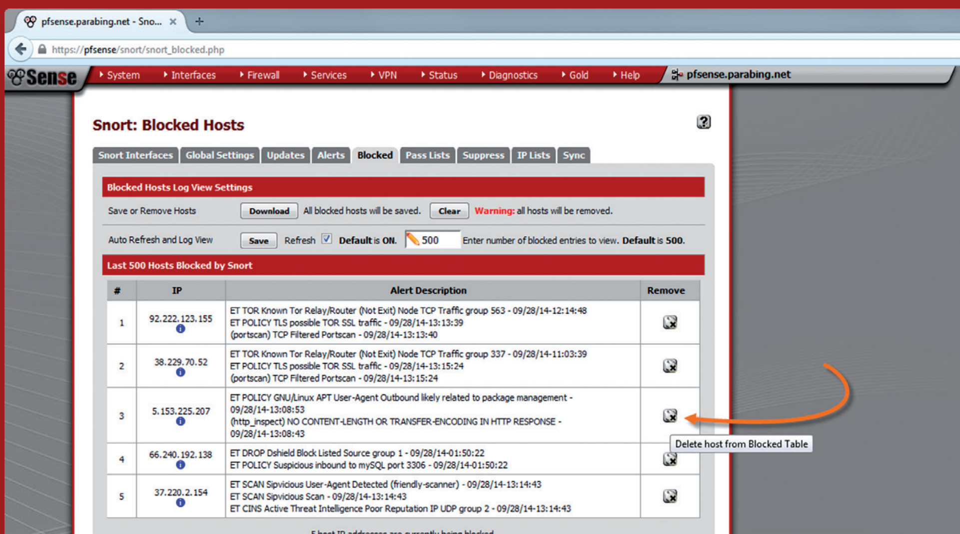
Ωπ! Το μπλοκαρισμένο host προφανώς κι αφορά σε mirrors του Raspbian, δηλαδή του λειτουργικού συστήματος που τρέχει το Raspberry Pi μας! Αυτός λοιπόν ήταν ο λόγος που αποτύγχανε το "sudo apt-get update" (true story).



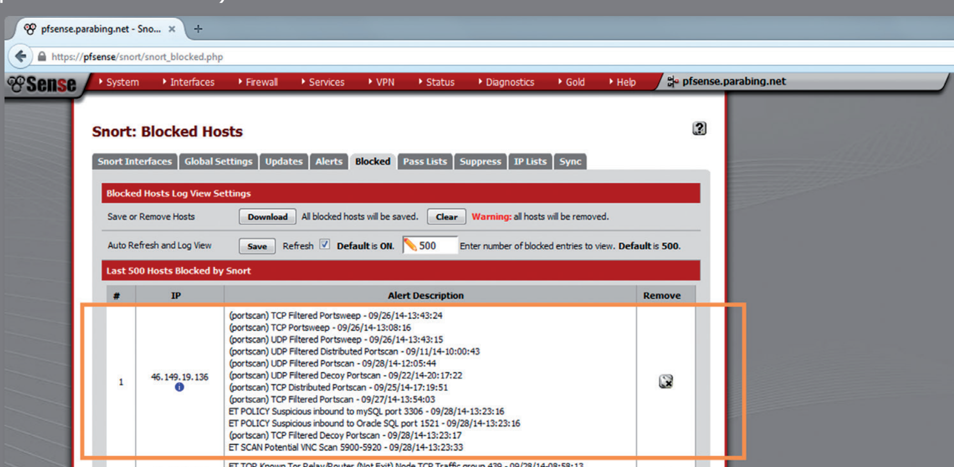
Αυτή τη φορά, αντί να ξεμπλοκάρουμε το host λέμε να απενεργοποιήσουμε τον κανόνα που οδήγησε στο μπλοκάρισμά του. Δεν θέλουμε να έχει παρόμοια θέματα το Pi μας στο μέλλον. Επίσης, εξαιτίας του ίδιου κανόνα έχει τύχει να διακοπεί η πρόσβασή μας στο `http://deltahacker.gr`, οπότε καταλαβαίνετε ότι μπορούμε να ζήσουμε και χωρίς αυτόν.



Απενεργοποιήσαμε τον κανόνα, αλλά αν θυμόσαστε τα offending hosts παραμένουν μπλοκαρισμένα για μία ώρα (αυτή είναι η προεπιλογή). Ευτυχώς, από τη λίστα των μπλοκαρισμένων ανά πάσα στιγμή μπορούμε εύκολα να διαγράφουμε όποιο host θέλουμε. Μια εναλλακτική λύση για την περίπτωση του mirrordirector.raspbian.org θα ήταν να βάλουμε το IP του (5.153.225.207) σε μια λίστα "pass list" (Services → Snort → Pass Lists). Τα hosts μιας τέτοιας λίστας δεν μπλοκάρονται ποτέ, ακόμη κι όταν στέλνουν πραγματικά κακόβουλο traffic στον router μας.



Να κι ένα άλλο μπλοκάρισμα, εξαιτίας port scanning αυτή τη φορά. Το 46.149.19.136 είναι το icebox.parabing.com και το scanning το κάναμε εμείς, για χάριν της επιστήμης :) Καταφύγαμε βεβαίως στο πανίσχυρο nmap, για το οποίο μπορείτε να διαβάσετε στα σχετικά άρθρα που φιλοξενούμε στο τεύχος 035 του deltaHacker (βλ. σελ. 24 και 52).




COOKIES
Έξοδος
Exit
ΑΓ. ΔΗΜΗ
ΠΟΥ ΕΙΣΑΙ ΡΕ, ΤΟΣΗ ΩΡΑ;
ΣΕ ΠΗΡΑ ΤΟΣΑ ΤΗΛΕΦΩΝΑ!
ΡΕ ΦΙΛΕ, ΕΧΕΙΣ ΔΙΚΙΟ, ΣΟΡΡΥ...
... ΟΠΩΣ ΒΛΕΠΕΙΣ ΑΦΗΣΑ ΤΟ ΣΜΑΡΤΦΟΝ ΣΤΟ ΣΠΙΤΙ...
ΠάΝΟΣ